



THE PUZZLE OF PAYMENTS SECURITY:

*Fitting the Pieces Together
to Protect the Retail Payments System*

An International Payments Policy Conference
Sponsored by the Federal Reserve Bank of Kansas City

Kansas City, Mo.
June 25-26, 2015

Copyright © 2015
Federal Reserve Bank of Kansas City
ISBN # 978-0-9744809-5-4

Contents

FOREWORD	vii
ESTHER L. GEORGE, President and Chief Executive Officer, Federal Reserve Bank of Kansas City	
CONTRIBUTORS	ix
CONFERENCE SUMMARY	xix
TERRI BRADFORD, Payments Research Specialist, Federal Reserve Bank of Kansas City	
OPENING REMARKS	1
KELLY J. DUBBERT, First Vice President and Chief Operating Officer, Federal Reserve Bank of Kansas City	
BUILDING A SAFER PAYMENT SYSTEM THROUGH COLLECTIVE ACTION	5
JEROME H. POWELL, Governor, Board of Governors of the Federal Reserve System	
GENERAL DISCUSSION	15
THE ECONOMICS OF RETAIL PAYMENTS SECURITY	21
FUMIKO HAYASHI, Senior Economist, Federal Reserve Bank of Kansas City	
TYLER MOORE, Assistant Professor, Southern Methodist University	
RICHARD J. SULLIVAN, Senior Economist, Federal Reserve Bank of Kansas City	

COMMENTARY	69
ADAM LEVITIN, Professor of Law, Georgetown University Law Center	
GENERAL DISCUSSION	79
MONITORING PAYMENT FRAUD: A KEY PIECE TO THE PUZZLE	89
ALEXANDRE STERVINO, Deputy Head, Payment Oversight Division, Banque de France	
COMMENTARY	105
CHRIS HAMILTON, Executive Director, Australian Payments Clearing Association	
GENERAL DISCUSSION	115
ACHIEVING A RESILIENT CYBER ECOSYSTEM: A WAY AHEAD Luncheon Keynote Address	125
PETER FONASH, Chief Technology Officer, Office of Cybersecurity and Communications, Department of Homeland Security	
GENERAL DISCUSSION	135
MANAGING THE THREATS TO DATA SECURITY	141
Moderator: TRACY KITTEN, Executive Editor, BankInfoSecurity and CUInfoSecurity, Information Security Media Group	
Panelists: MARK CARNEY, Vice President, Strategic Programs, FireMon	
ROBERT CARR, Chief Executive Officer, Heartland Payment Systems	
LIZ GARNER, Vice President, Merchant Advisory Group	

VERNON MARSHALL, Functional Risk Officer,
American Express

GENERAL DISCUSSION 161

DEVALUING DATA: IF THE SYSTEM CANNOT BE MADE SECURE, CAN THE INFORMATION BE MADE WORTHLESS? 171

Moderator: **MARIANNE CROWE**, Vice President,
Federal Reserve Bank of Boston

Panelists: **STEVE SCHMALZ**, Solution Architect,
RSA, The Security Division of EMC

RADHA SUVARNA, Managing Director,
Head of U.S. Emerging Payments, Citi Cards,
Citibank
and Member,
Tokenization Subcommittee, X9

MADHU VASU, Senior Director, Innovation and Strategic Partnerships,
Visa Inc.

BRANDEN R. WILLIAMS, Chief Technology Officer, Cyber Security Solutions,
First Data Corp.

GENERAL DISCUSSION 189

ROLE OF INDUSTRY COLLABORATION IN PAYMENTS SYSTEM SECURITY 195

Moderator: **JONATHAN WILLIAMS**, Director of Strategic Development,
Experian

Panelists: **CHARLES BRETZ**, Director of Payments Risk,
Financial Services Information Sharing and Analysis Center

SANDRA KENNEDY, President,
Retail Industry Leaders Association
and Co-Chair,
Merchant Financial Services Cybersecurity Partnership

NANCY O'MALLEY, Chief Payment System Integrity Officer,
MasterCard Worldwide
and Member,
Payments Security Task Force

LIZ VOTAW, Senior Vice President, OmniChannel Authentication Strategy,
Bank of America
and Board of Directors,
Fast IDentity Online Alliance

GENERAL DISCUSSION 217

ROLE OF GOVERNMENT IN PAYMENTS SYSTEM SECURITY 227

Moderator: **GORDON WERKEMA**, Payments Strategy Director,
Federal Reserve Bank of Chicago

Panelists: **ANJAN MUKHERJEE**, Counselor to the Secretary and Deputy
Assistant Secretary for Financial Institutions,
U.S. Department of the Treasury

CHRISSANTHOS TSILIBERDIS, Senior Market Infrastructure Expert,
European Central Bank

COEN VOORMEULEN, Director of the Cash and Payments Division,
De Nederlandsche Bank
and Co-Chair,
Working Group for Cyber Resilience, BIS

GENERAL DISCUSSION 241

CLOSING REMARKS 249

ESTHER L. GEORGE, President and Chief Executive Officer,
Federal Reserve Bank of Kansas City

CONFERENCE ATTENDEES 253

Foreword



The retail payments system in the United States is under duress as never before. Regular cyberattacks and large-scale data breaches have exposed the sensitive information of millions of consumers and resulted in fraudulent payment transactions totaling billions of dollars. These attacks are perpetrated by adversaries that are motivated and well-funded. They have access to an adaptable arsenal of cyberweapons that helps them exploit gaps in payments system security.

The Federal Reserve, as the nation's central bank, has a keen interest in promoting and fostering the security of the payments system in the United States, and is leveraging its roles as an operator and an overseer within the payments system to help usher in important improvements for payments security.

To that end, the Federal Reserve Bank of Kansas City brought together payments system participants, academics and policymakers to exchange thoughts and views on payments security and fraud as matters of importance for preserving public confidence in payment systems around the globe. More than 120 industry leaders met June 25-26 in Kansas City, Mo., for the bank's fifth international payments policy conference, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System."

Subjects addressed included the underlying economics of payments security; how to best allocate resources between preventing, detecting and responding to cyberthreats; how to secure or, if necessary, devalue sensitive information; and the roles of private industry and government in securing the payments system. If we are to be successful at making the payments system more secure and efficient, we will need the efforts of all players involved—private industry, academics, central banks and policymakers.

Some of the discussion focused on the role of the Federal Reserve in these efforts. The Fed always has had a leadership role in advancing the safety, efficiency and accessibility of the nation's payments system. A century after its founding, the Fed has established two task forces to address today's challenges. One task force will identify and evaluate approaches for putting in place a safe, faster payments capability in the United States; the other will provide input on security aspects of a faster payments capability and serve as a forum to advise the Fed to identify and address actions that can be taken by payments system participants as a group or by the Federal Reserve System.

We sincerely thank the conference participants for their contributions to enhancing our understanding of how best to piece together the puzzle of payments security. I also thank members of the staff of the Federal Reserve Bank of Kansas City who helped plan and arrange the conference.

A handwritten signature in black ink, reading "Esther L. George". The signature is written in a cursive, flowing style with a large initial "E".

Esther L. George
President and Chief Executive Officer
Federal Reserve Bank of Kansas City

Contributors



Charles Bretz

Director of Payment Risk, Financial Services Information Sharing and Analysis Center

Mr. Bretz supports FS-ISAC's Payment Processor Information Sharing Council and Payment Risk Council. In this role he coordinates the Cyber Attack Against the Payment Process exercises.

Mr. Bretz has more than 20 years of executive management experience with a major regional U.S. bank in online sales, online service delivery, mobile banking and bank cards. He has been a member of the board of directors of NACHA-The Electronic Payments Association.

Mark Carney

Vice President, Strategic Programs, FireMon

Mr. Carney is involved with strategic programs that affect companywide initiatives surrounding product development, sales, marketing, professional services, channel partnerships and business operations. Prior to joining FireMon, he was vice president of strategic services at FishNet Security, where he built and led a national group of security advisers.

Mr. Carney spent more than 12 years at FishNet and was the primary executive liaison between FishNet and the card brand Qualified Incident Response Assessor/Qualified Forensics Investigator programs, as well as the PCI Security Standards Council and Forensic Investigation Program around post data breach engagements and reporting. He is a frequent speaker at security conferences and has published several articles.

Robert Carr

Chief Executive Officer, Heartland Payment Systems

Mr. Carr co-founded Heartland Payment Systems in 1997 and has been chief executive officer of the company since 2000. He also is chairman and CEO of Carr Holdings LLC. Heartland, one of the world's largest payments processing companies, has grown from 25 employees in 1997 to more than 3,000.

Mr. Carr started his career as a professor, president of the faculty and director of the computer center at Parkland College in Champaign, Ill., before moving to the Bank of Illinois. In 1987 he founded Credit Card Software Systems Inc., which specialized in the travel and entertainment industries. The MidWest Acquirers Association recognized Mr. Carr in 2003 with its first "Lifetime Achievement Award." Ernst and Young recognized him with its "Entrepreneur of the Year Award" in 2004 and 2007.

Marianne Crowe

Vice President, Federal Reserve Bank of Boston

Ms. Crowe is a vice president in Treasury and Financial Services, where she serves as the Mobile Payments Project manager and payments liaison to the Consumer Payments Research Center.

Ms. Crowe's previous roles at the Boston Fed include vice president/project manager in the Consumer Payments Research Center, assistant vice president of business development, the National Image Archive service and the Boston check operations. Prior to joining the Fed in 2000, she worked at BankBoston. Ms. Crowe has been a member of the FSTC mobile payments workgroup and the NACHA Internet Council.

Kelly J. Dubbert

First Vice President and Chief Operating Officer, Federal Reserve Bank of Kansas City

Mr. Dubbert is responsible for the Bank's operations and budget administration. Among the areas for which he has direct oversight are Information Technology, Financial Services and Check Automation Services. Previously, Mr. Dubbert was senior vice president and chief information officer over the Bank's Information Technology Division.

Mr. Dubbert has participated in numerous Federal Reserve System information technology leadership groups and was co-chair of the Technology Services Council, a group representing all Reserve Bank and national business line CIOs. He has also served as a liaison member to the Business Technology Council and the Information Technology Oversight Committee.

Peter Fonash

*Chief Technology Officer, Office of Cybersecurity and Communications,
Department of Homeland Security*

Mr. Fonash is chief technology officer for the Office of Cybersecurity and Communications in the Department of Homeland Security. He has been a member of the Senior Executive Service since 1998. He assumed his current role after serving as deputy manager and director of the National Communications System.

Mr. Fonash also was the chief with the Defense Information System Agency Joint Combat Support Applications Division. Prior to working for the federal government, Mr. Fonash worked for AT&T and Burroughs Corp. (Unisys).

Liz Garner

Vice President, Merchant Advisory Group

Ms. Garner focuses on industry affairs and advancing the Merchant Advisory Group's mission of positive change in payments through collaboration.

Ms. Garner previously was director of commerce and entrepreneurship at the National Restaurant Association, where she represented the restaurant and foodservice industry before Congress and federal regulatory agencies on issues including retail and mobile payments, data security and emerging technologies. She also was director of government relations for the Food Marketing Institute (FMI) and was the staff liaison to the FMI Electronic Payments Committee.

Esther L. George

President and Chief Executive Officer, Federal Reserve Bank of Kansas City

Ms. George has been president and CEO of the Bank since 2011. She is a member of the Federal Open Market Committee, which has authority over U.S. monetary policy. She also hosts the Bank's annual Economic Policy Symposium in Jackson Hole, Wyo. Prior to her appointment as president, Ms. George had been the Bank's chief operating officer since August 2009.

Ms. George joined the Bank in 1982 and has worked much of her career in the Division of Supervision and Risk Management, including 10 years as the Tenth Federal Reserve District's chief regulator. In that capacity, she was directly involved in the Tenth District's banking supervision and discount window lending activities during the banking crisis of the 1980s and post-9/11.

Chris Hamilton

Executive Director, Australian Payments Clearing Association

Mr. Hamilton has been executive director and chief executive officer of the Australian Payments Clearing Association (APCA) since 2006. APCA is a

self-regulatory body and industry association for Australian payments. It provides the venue for banks, non-bank financial institutions, large merchants and many others engaged in the Australian payments system to work together on its efficient operation and future enhancement.

Prior to this appointment, Mr. Hamilton spent 11 years at the Australian Stock Exchange (ASX) in a variety of roles. He worked at the ASX throughout the transition from a stockbrokers' mutual into the world's first self-listed stock exchange.

Fumiko Hayashi

Senior Economist, Federal Reserve Bank of Kansas City

Ms. Hayashi is a senior economist in the Payments System Research Department at the Federal Reserve Bank of Kansas City. Since joining the Federal Reserve in 2001, Ms. Hayashi has published studies on the ATM and debit card industry, regulatory developments around interchange fees and card network rules, consumer payment choice, mobile payments and nonbanks in the payments system. Her current research focuses on the use of general purpose reloadable prepaid cards, implications of recent regulations and litigations in the payment card industry for industry participants and end users, and the security of the payments system.

Prior to joining the Bank, Ms. Hayashi conducted research examining consumer savings and long-term care insurance, social security reform in Japan and nursing home markets in the United States.

Sandra Kennedy

*Co-Chair, Merchant Financial Services Cybersecurity Partnership;
President, Retail Industry Leaders Association*

Ms. Kennedy is co-chair of the partnership, which consists of payments system organizations such as retailers, banks, card companies and security and technology vendors. The partnership recently released recommendations outlining new ways companies can use technology to minimize data theft and reduce the value of stolen payment information.

Ms. Kennedy also is president of the Retail Industry Leaders Association (RILA), a position she has had since 2002. She also is a member of the White House Advisory Committee for Trade Policy and Negotiations. Prior to joining RILA, Ms. Kennedy was director of the Leadership Dialogue Series for Accenture and was senior vice president of membership services for the National Retail Federation.

Tracy Kitten

Executive Editor, BankInfoSecurity and CUInfoSecurity, Information Security Media Group

Ms. Kitten has more than 16 years of experience as a journalist and has covered the financial sector for the last nine years. Since 2010, she has been part of Information Security Media Group, where she is executive editor of BankInfoSecurity and CUInfoSecurity.

Ms. Kitten previously covered the financial self-service industry as the senior editor of ATMmarketplace, part of Networld Media Group. She has been a regular speaker at domestic and international conferences.

Adam Levitin

Professor of Law, Georgetown University Law Center

Mr. Levitin teaches courses in consumer finance, structured finance, contracts, bankruptcy and commercial law. He also is a member of the Consumer Financial Protection Bureau's Consumer Advisory Board. He previously was the Bruce W. Nichols Visiting Professor of Law at Harvard Law School, the Robert Zinman Scholar in Residence at the American Bankruptcy Institute and Special Counsel to the Congressional Oversight Panel supervising the Troubled Asset Relief Program.

Before joining the Georgetown faculty, Mr. Levitin practiced in the Business Finance & Restructuring Department of Weil, Gotshal & Manges LLP in New York. Among other honors, in 2013 Mr. Levitin received the American Law Institute's Young Scholar's Medal.

Vernon Marshall

Functional Risk Officer, American Express

Mr. Marshall leads a team of more than 250 risk professionals and is responsible for decision science for all of the company's consumer and commercial products, fraud protection, central rating and underwriting and global credit bureau functions.

Mr. Marshall has been with American Express for more than 25 years and has had various positions in risk management and technologies in the United States and Europe. Prior to his current position, Mr. Marshall was chief credit officer for OPEN, Global Corporate Payments and Global Merchant Services and chaired the Institutional Risk Committee.

Tyler Moore

Assistant Professor, Southern Methodist University

Mr. Moore is an assistant professor of computer science and engineering at Southern Methodist University. His research focuses on the economics of information security, the study of electronic crime and the development of policy for strengthening security. He directs the Security Economics Lab within the High Assurance Computing and Networking Labs, a research group of faculty and students working in areas related to security.

Mr. Moore was a director and vice president of the International Financial Cryptography Association from 2011 to 2014. He also is editor in chief of the new *Journal of Cybersecurity*.

Anjan Mukherjee

Counselor to the Secretary and Deputy Assistant Secretary for Financial Institutions, U.S. Department of the Treasury

Mr. Mukherjee is counselor to the secretary and deputy assistant secretary for financial institutions. He is an adviser on matters related to financial institutions and markets, and oversees the Office of Financial Institutions Policy, the Office of Critical Infrastructure Protection and the Federal Insurance Office.

Prior to joining the Treasury, Mr. Mukherjee was a senior managing director at Blackstone Group LP, an investment management firm, where he served on the investment committee. Mr. Mukherjee had posts at Thomas H. Lee Co., Morgan Stanley and the U.S. Department of Education prior to joining Blackstone in 2001. In 2008, he was part of President Barack Obama's Transition Team, focusing on matters of economics and international trade.

Nancy O'Malley

*Chief Payment System Integrity Officer, MasterCard Worldwide;
Member, Payments Security Task Force*

Ms. O'Malley is responsible for the development and execution of information and network security functions and the detection and prevention of global fraud. Her responsibilities include: providing strategic information and advice to inform MasterCard safety and security strategy; regulatory relations and strategy as it relates to fraud; management of the chief information security officer function; developing new fraud products, solutions and services; and guiding the development and adoption of industry standards to prevent fraud including mobile strategy, tokenization, POS terminals, ATMs and payment cards.

Ms. O'Malley is a member of the Payments Security Task Force, a cross-industry group focused on driving executive-level discussion to enhance security of the payments system.

Jerome H. Powell

Governor, Board of Governors of the Federal Reserve System

Mr. Powell joined the Board of Governors in 2012, filling an unexpired term. He was reappointed in 2014, for a term ending in 2028. Prior to his appointment to the Board, Mr. Powell was a visiting scholar at the Bipartisan Policy Center in Washington, D.C., where he focused on federal and state fiscal issues. From 1997 through 2005, Mr. Powell was a partner at The Carlyle Group.

Mr. Powell served as an assistant secretary and as undersecretary of the Treasury under President George H.W. Bush, with responsibility for policy on financial institutions, the Treasury debt market and related areas. He previously was a lawyer and investment banker in New York City.

Steve Schmalz

Solution Architect, RSA, The Security Division of EMC

Mr. Schmalz assists organizations in understanding their security architecture needs and how RSA's security products can help protect their critical infrastructure. Mr. Schmalz has spoken at multiple venues on topics ranging from standards compliance to cryptography. He is a longtime participant in ASC X9 and is a member of X9 F6, where he is technical editor for a new tokenization standard.

Before joining RSA, he was director of business development at Quantrad, a biometrics vendor. He also worked for the National Security Agency as a cryptographic mathematician.

Alexandre Stervinou

Deputy Head, Payment Oversight Division, Banque de France

Mr. Stervinou mostly deals with policy and oversight matters both at national and European levels. His division, created in 2002, has developed expertise in payment fraud and security and is in charge of issuing recommendations to payment service providers to improve the security of retail payments. He is also secretary of the Observatory for Payment Card Security and secretary of the national committee in charge of the European SEPA project.

Mr. Stervinou represents Banque de France at the European forum on the Security of Retail Payments (SecuRe Pay). Prior to this role, he had various private-sector positions in which he focused on security solutions mainly for the financial services and telecom industries.

Richard J. Sullivan

Senior Economist, Federal Reserve Bank of Kansas City

Since joining the Federal Reserve in 1994, Mr. Sullivan has completed a number of studies on the retail payments industry and on the banking industry. Topics of recent publications include the effect of computer chip payment cards on payment fraud and how regulation of interchange fees on debit cards affects the fee structure of checking accounts. His research has appeared in Federal Reserve publications and in academic journals such as the *Journal of Financial Intermediation*, *Journal of Banking and Finance*, *Economica*, and the *Journal of Economic History*. He is on the editorial board of the *Workshop on the Economics of Information Security*.

Prior to joining the Bank, Mr. Sullivan taught at Holy Cross College and the University of Colorado.

Radha Suvarna

Managing Director, Head of U.S. Emerging Payments, Citi Cards, Citibank; Member, Tokenization Subcommittee, X9

Mr. Suvarna leads the Emerging Payments group, which is responsible for development of emerging payments strategies and solutions for the credit card business, including mobile payments, proximity and remote commerce solutions. He also is a member of the X9 Tokenization Subcommittee.

Mr. Suvarna has a diversified background in credit cards, payments and managing various functions and businesses, including emerging payments, new product development and credit cards product and portfolio management across multiple countries.

Chrissanthos Tsiliberdis

Senior Market Infrastructure Expert, European Central Bank

Mr. Tsiliberdis is a member of the Oversight Division, where he has been responsible for overseeing various payment systems (CLS, EURO1/STEP1/STEP2), card payment schemes, payment instruments (SEPA Direct Debit and Credit schemes, PayPal, etc.) and SWIFT. He also is the responsible expert for operational risk oversight policy issues and coordinated the drafting of Eurosystem oversight policies on business continuity for SIPS, the oversight standards for card payment schemes.

Previously, he was involved in the cooperative oversight arrangements for the oversight of the card payment schemes, CLS and the implementation of the Eurosystem's High Level Group on SWIFT Oversight, of which he is the secretary. He has represented the ECB in various CPMI-IOSCO working groups such as the legal entity identification implementation group and the cyberresilience group.

Madhu Vasu

Senior Director, Innovation and Strategic Partnerships, Visa Inc.

Ms. Vasu has 18 years of experience in the payments and business intelligence industries, catering to financial services. Her focus has been on initiating early stage concepts and building solutions in e-commerce and the mobile space both in the United States and emerging markets.

Ms. Vasu previously was a senior consultant at MicroStrategy for four years and a consultant for two years at Procter & Gamble.

Coen Voormeulen

*Director of the Cash and Payments Division, De Nederlandsche Bank;
Co-Chair, Working Group for Cyber Resilience, BIS*

Mr. Voormeulen is responsible for bank notes and noncash in terms of policy, operations and oversight at De Nederlandsche Bank. He is a member of the Committee for Payments Systems and Market Infrastructures (CPMI) and co-chair of its Working Group for Cyber Resilience.

Mr. Voormeulen formerly was chair of CPMI's cybersecurity working group, a member of the Payments and Settlements Systems Committee of the European System of Central Banks and chair of the Dutch National SEPA Task Force. He also is a member of the board of the Dutch Payments Society and of the Supervisory Board of Geldservice Nederland, a company that processes bank notes.

Liz Votaw

*Senior Vice President, Bank of America;
Board of Directors, Fast IDentity Online Alliance*

Ms. Votaw is a senior vice president in OmniChannel Authentication Strategy, where she develops and drives customer-focused authentication strategies to deliver secure and convenient banking. Ms. Votaw also represents Bank of America as a member of the board for the Fast IDentity Online Alliance.

Ms. Votaw previously worked in Innovation at Bank of America, developing concepts across the enterprise, and is the inventor on 12 granted patents, with 25 patents pending. Her career at the bank includes 25 years of leadership positions in operations, technology, fraud prevention, risk and innovation.

Gordon Werkema

Payments Strategy Director, Federal Reserve Bank of Chicago

Mr. Werkema is responsible for leading major payment system improvement initiatives described in the Federal Reserve's recently published paper "Strategies for Improving the U.S. Payment System." In his 34-year career,

Mr. Werkema has been first vice president and chief operating officer of the Federal Reserve Bank of Chicago and executive vice president of the Federal Reserve Bank of San Francisco.

Mr. Werkema was a member of the executive team that developed the strategies paper. He will lead the Federal Reserve's strategies related to faster payments, payments security and stakeholder engagement, collaborating with the Federal Reserve's current financial services product leaders to execute the full complement of strategies outlined in the paper.

Branden R. Williams

Chief Technology Officer, Cyber Security Solutions, First Data Corp.

Mr. Williams has almost 20 years of experience in business strategy, information technology and security and payments, finding solutions that move companies ahead while reducing risk. He is a co-author of three books on PCI compliance.

Mr. Williams previously was director of consulting at VeriSign and a chief technology officer at RSA, The Security Division of EMC. He also has been a member of the PCI Board of Advisors.

Jonathan Williams

Director of Strategic Development, Experian

Mr. Williams is a strategist with a broad background in payments, networking and telecommunications, real-time systems, security, encryption and authentication. At Experian, he is responsible for innovation, industry relations and strategic projects for the identity and fraud group. He speaks at industry conferences worldwide.

Mr. Williams previously was European business development manager for Fujitsu Telecom and had engineering and IT roles at British Aerospace (now BAE Systems), the University of Cambridge and Advanced Telecommunications Modules Ltd. He also had senior marketing roles at Virata Corp. and Content Technologies (now Clearswift).

Conference Summary



Terri Bradford

I. Introduction

Cyberattacks and large-scale data breaches that expose the sensitive information of millions of consumers and result in billions of dollars of fraudulent payment transactions have elevated payments security to a forefront issue. In 2014 there were 783 data breaches in the United States that exposed more than 85 million records.¹ Although U.S. retail payment systems do not receive the same scrutiny as large-value payment systems, the public expects them to work without fail every day; their smooth functioning is critical to the public's confidence in new and more efficient ways to pay. As a consequence, payment participants—end users who make payments, financial institutions and nonbanks that provide payment services, and networks and service providers that process payments—all have considerable incentive to secure payments and deter fraud.

As industry participants look for ways to improve payments security, there are many issues with which to contend. Among them are key policy questions such as: What economic principles underlie the determinants of payments security? What options are available to better align incentives of payments stakeholders? How best are resources allocated between preventing, detecting and responding to payments security threats? How should the changing threat landscape affect the ways in which sensitive information is secured and used for retail payments? What are the roles of private players and public authorities, given coordination problems and challenges in obtaining data on payments fraud and other security indicators?

These and other key policy questions create a puzzle for the myriad of payments participants to solve, and formed the motivation for the Federal Reserve Bank of Kansas City's fifth international policy conference titled, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the

Retail Payments System.” The conference was hosted on June 25-26, 2015, in Kansas City, Mo. During six sessions and two keynote addresses, more than 120 payments system participants and observers exchanged thoughts and views on payments security and fraud as matters of importance for preserving public confidence in payment systems around the globe.

Each session focused on one of the motivating policy questions. The following summarizes each session of the conference, highlighting key insights, areas of agreement and points of contention.

II. Opening Remarks: An Opportunity to Consider Solutions

Kelly J. Dubbert, first vice president and chief operating officer of the Federal Reserve Bank of Kansas City, opened the conference by acknowledging the complexity involved in securing the retail payments system. Dubbert noted that while security has never been simple, the issue has become more complex because of the pace of growth and innovation within the payments system and the many participants, technologies and issues involved. The flow of goods and services relies on a well-functioning payments system, and security has always been a key component of those transactions, which are a critical part of the economy. Dubbert added that while central banks have an important role in assuring public confidence in the system, more broadly, payments security requires the active engagement of the spectrum of payments system participants. As the central bank for the United States, and as both an operator of retail payment systems and an overseer of the financial institutions that many use to access the payments system, the Federal Reserve is in a unique position to promote the involvement of the respective industry segments. Dubbert said the puzzle of payments security we face today cannot be solved by working separately. He urged participants to use the conference as an opportunity to consider how available solutions can be leveraged collectively to address the payment system’s broader challenges.

III. Keynote Address: Building a Safer Payments System through Collective Action

Federal Reserve Gov. Jerome H. Powell provided the conference keynote in which he described the importance of payments participants working together to maintain and enhance a safe and secure payments system. He discussed the Federal Reserve’s current efforts to improve the speed,

efficiency and security of the payments system, pointing to the consultation paper published in 2013 that sought public input on ways to make the U.S. payments system safer, more accessible, faster and more efficient from end-to-end; the release of a second paper in 2015 that outlined strategies for improving the U.S. payments system, and the subsequent establishment of two task forces: one for faster payments and one for payments security.

Powell then stressed that payment system participants must work together by participating in coordinated efforts to improve the payments system. He noted that the market should be the primary driver of change, and government should avoid stifling healthy innovation. During the balance of his remarks he spoke about four actions all payments participants need to take with respect to payments security. The first is to embrace safe innovation, while prudently managing new risks that may be introduced by new technologies. The second is to implement preventative tools—defensive tactics—because it is not a matter of if there will be an attack, but rather when. The third is to complement prevention with a comprehensive payment security plan. And the fourth is to collectively educate consumers to empower them to safely use financial products.

Concluding his remarks, Powell asked for the support of payments system participants in building a safer and more efficient payments system. He noted that a high level of engagement will be critical and encouraged participation in one of the Federal Reserve's task forces and in providing feedback.

During the question and answer period, participants asked Powell about his reaction to the breach at the Office of Personnel Management (OPM), and about the role of the Federal Reserve: should it use its dual roles of operator and regulator to drive which aspects of security are put in place by market players; is there really a universal case favoring faster payments; can it really help the United States catch up to the rest of the world? Powell indicated the Fed was looking closely at the OPM breach, trying to understand what happened and how that information can be used to safeguard the System's employees. He added that while the Fed does have regulatory and supervisory authority over banks, its plenary authority does not extend over the financial system or the whole payments system. As for faster payments, Powell agreed consumers and businesses want faster payments but that not every payment needs to be made instantaneously. Innovation, Powell said, and a more flexible economy will enable the United States to catch up and pass the rest of the world.

IV. The Economics of Payments Security

In the opening session, “The Economics of Payments Security,” Tyler Moore of Southern Methodist University presented a paper he co-authored with Fumiko Hayashi and Richard J. Sullivan, both from the Federal Reserve Bank of Kansas City, that discussed how economics can help to better understand the dynamics of retail payments security and explain why the payments system is not moving as quickly as it might to better, more secure technologies. Moore outlined the basic economic principles that characterize retail payments markets; network externalities, two-sided markets and economies of scale and scope, as well as principles that pertain particularly to payments security; jointly produced goods, competition for the market, asymmetric information, moral hazard and trade-offs that occur between information sharing and privacy. After explaining how these principles are related to challenges to effective payments security, Moore discussed how the game theory approach can be used to evaluate and construct strategies that can achieve socially desirable levels of payments security.

To illustrate the value of modeling payments security scenarios using game theory, Moore offered four case studies where incentives appear insufficient to adequately secure payments. The first concerned fraud in card-not-present (CNP) payments, such as online payments where the card is not physically presented to a merchant. The second case study illustrated inadequate protection of sensitive payment data that is useful for committing payment fraud. The third and fourth case studies were mobile payments and cryptocurrencies, both of which are potentially more secure than existing payment methods but also face additional challenges, such as adoption by end users and establishment of control structures that ensure integrity of the overall payments ecosystem. Moore used these case studies to demonstrate that the interdependence in modern payments systems poses significant challenges to improving security, which may make the status quo appear satisfactory.

Moore noted that in each case study, leadership of collaborative efforts is important to appropriately modify games of collaboration, and thus achieve socially desirable levels of payments security. More specifically, leadership should modify games of coordination so that the best-positioned payment participant has enough incentive to balance the incremental costs of security against the incremental reduction in fraud, data breaches and other security incidents. He offered that effective leadership requires strong

commitment, credibility and an understanding of conflicts of interests across various parties. He said these attributes help leaders effectively reconcile the conflicts of interests and build trust among involved parties. That trust then may lead to collaboration on rules or guidelines concerning property rights, distribution of costs and liability, or limited available options to each party. The attributes also help leaders improve involved parties' expectations for prospects and outcomes of collaboration and thereby induce these parties to collaborate effectively.

Moore concluded that the biggest challenges to adopting socially desirable levels of payments security are economic not technical. Competing interests and incentives may inhibit adoption of more secure technologies. As a result, coordination among stakeholders is essential, and game theory can uncover superior outcomes as well as strategies to attain them. Moore noted that public authorities and academics, due to long-term vision and societal outlook, can help overcome barriers to collaboration.

Adam Levitin of the Georgetown University Law Center was Moore's discussant. Levitin agreed that game theory provides a foundation from which the understudied area of payments security economics can begin to be better approached, but that externalities and spillover effects to third parties are not accounted for in the application of the theory. Levitin critiqued the paper's assumptions about knowledge, causation, the bilateral nature of the game and the use of binary choice; however, he acknowledged that the game theory assumptions are valuable in pointing out where to focus payments security policy. Levitin suggested that the policy agenda for payment security should focus on better data collection, better antitrust enforcement and reducing externalities without creating unintended consequences.

Levitin also said private or public ordering—self regulation or government intervention—can be used to achieve the goal of greater payments security in different contexts. He noted that neither is perfect. There are issues with private ordering; and it is less clear how good of a result can be achieved with public ordering. That said, Levitin observed that public ordering is the direction in which payments security policy appears to be gravitating; driven in large part by headlines about data breaches, which are creating legislative and regulatory interest and national security concerns.

Responding first to Levitin's commentary, Moore opened the discussion period by agreeing that game theory does not account for externalities

and that the models ignore them. He added that the real conversation of externalities takes place in the public/social optimum, motivating the need for greater public oversight and involvement. However, because it is doubtful public authorities will come up with better solutions, it is important that the private sector remain engaged. Questions from the audience ranged from whether Bitcoin can be a long-term viable retail payment system to whether zero fraud in the payments system is the correct policy goal. Levitin noted that it is hard to see Bitcoin being attractive in stable economies; but the underlying blockchain technology could be valuable. Moore added there is technical innovation with a distributed secure system that could be available. Levitin and Moore both argued against the concept of zero fraud being attainable, with Levitin favoring getting to a point where the marginal losses due to fraud equal the marginal cost of fraud prevention.

Moore and Levitin concluded that while game theory works well to analyze an idealized version of the world there is not any one correct security setting for all payments, but there are some policy principles that should be pursued. First, data collection in standardized forms is a key to applying game theory to the real world. Second, from a policy perspective, ideal security strategies should be broad in scope and meet longer-term needs rather than achieve a single security improvement. Third, to encourage participation in such strategies, it is important that costs and benefits be fairly distributed among participants.

V. Monitoring Payment Fraud: A Key Piece to the Puzzle

In the session “Monitoring Payment Fraud: A Key Piece to the Puzzle,” Alexandre Stervinou of the Banque de France’s Observatory for Payment Card Security and Chris Hamilton of the Australian Payments Clearing Association (APCA) shared insights from their experiences collecting and analyzing payments data and data facilitating payment security improvements.²

Stervinou said the Observatory monitors security measures adopted by issuers and merchants, establishes aggregate fraud statistics and maintains a technology watch for payment cards. The Observatory started collecting data to better understand fraud rates, its prevalence and where it originated and produced its first annual report of fraud data in 2006. Stervinou said that from the information the Observatory has gathered, it has generated fraud statistics, identified trends, made recommendations, and closely monitored security measures deployed by issuers/banks and merchants.

One outcome of the Observatory's data collection efforts has been a push for stronger customer authentication in online transactions. Stervinou said the Observatory strongly advocated use of two-factor authentication and encouraged the use of 3D Secure.³ The Observatory worked to convince involved parties that there were incentives for adopting these stronger security methods and allowed for a risk-based approach for deploying stronger authentication. The Observatory recognized that for its efforts to be most effective it needed a broader approach, one that was not "French-only." As a result, it supported the emergence of a European forum for supervisors and central bankers through which there was a successful legislative push to require strong two-factor authentication. Stervinou added that the European Banking Authority released guidelines in December 2014 on securing online payments across the European Union (EU), including an implementation deadline of Aug. 1, 2015, for EU companies to begin research and deployment.

Hamilton offered a private-sector perspective, noting that 10 years ago, after concluding the lack of investment in payment security was partly due to the lack of appropriate data, APCA began collecting data to better understand fraud rates and prevalence, the consequence of fraud and the threat matrix. Hamilton said data is essential for risk management capability and for enhancing public debate when arguing for security improvements. With the data, an impact analysis can identify what happens when fraud occurs—who ultimately bears the losses, what are the real costs and the cost of implementing new security technologies. Hamilton said reporting requires cooperation, which has helped participating organizations manage their own fraud. Hamilton noted that APCA has found that, in contrast to the approach taken by the Observatory, data capture and reporting are better done when voluntary than when required by regulation. It is more cost effective and also enables a greater focus on industry needs; however, he conceded that the quality of the data has room to improve. Hamilton added that APCA also shares the information with the public to broaden the awareness of fraud and its prevention.

Stervinou, responding to Hamilton's commentary, said the decision to intervene in security and collect data are two separate things. Banque de France wanted to intervene to improve security, but to determine the appropriate intervention and issue recommendations, he said, the central bank had to have the necessary data. Stervinou added it is important to find

the right balance between regulation and innovation by market players. As a public authority the Banque de France offered neutrality, which is very important because security must not be a competitive issue.

Participants' questions ranged from why the United States is undergoing an expensive conversion to Europay, MasterCard and Visa (EMV) chip payment cards without mandating personal identification numbers (PINs) to whether collecting and publishing fraud data has the unintended consequence of increasing consumers' fear of fraud. Stervinou and Hamilton agreed a better approach in the United States would be chip and PIN; Stervinou added "chip is half the way through; it is a good half, but it is still half the way through." Hamilton said the annual reports Australia releases on fraud have actually reduced consumers' fears about fraud. Stervinou added that the release of fraud statistics is a good opportunity to remind consumers of their responsibility to help safeguard their information.

Stervinou and Hamilton agreed that data collection is essential to understanding rates, the prevalence and origination of fraud, and facilitates an understanding of the real costs of fraud and security breaches. Hamilton said ultimately, what can be measured can be managed and attempting to choose between private action and public intervention is likely a false dichotomy. Stervinou added the private and public sectors need to work in tandem because fraud and payments security are everyone's concern. They concurred that a collaborative approach to collecting data on fraud and payments security incidents is most beneficial. Ultimately, facts will make for better public debate about how best to allocate resources.

VI. Luncheon Keynote: Achieving a Resilient Cyber Ecosystem: A Way Ahead

Peter Fonash of the U.S. Department of Homeland Security (DHS) spoke about the cyber ecosystem and the efforts under way at DHS to raise the level of cybersecurity for the whole country. Fonash explained because cybersecurity is everyone's concern, raising the overall security of the ecosystem is needed. He provided evidence that 10 years ago adversaries were more effective in attacking the cyber ecosystem than the industry in detecting intrusions and the gap has grown. He said the Internet of Things will drive enormous growth in the scale and scope of potential cybersecurity intrusions; expanding devices accessible via the Internet—including cars, refrigerators, home heating systems—that are not actually under anyone's security control

will make it difficult to effectively provide security for controlled enterprises. Moreover, he observed organizations' budgets today are mostly flat or decreasing and staffing levels are insufficient to address the problem.

Fonash said the effectiveness of cybersecurity needs to be improved. The security analysts today have incomplete knowledge of their individual organizations and what is happening in the Internet in general, but they need to become more productive. The time to detect and respond to a cybersecurity intrusion needs to be reduced from months to days or minutes. Although there are a lot of innovations in the research community, better management of the process of inserting innovations into existing systems is needed. There needs to be a move away from the model of treating all data as equal to a risk-based framework.

Fonash said these improvements can be accomplished with industry consensus on interoperability, automation, trust and information sharing. He defined interoperability as the integration of tools into a tool set with common semantics and syntax of data so as to provide security analysts with a common understanding of what the data mean without spending too much time reconciling data that only appear to be different. Interoperability enables automated courses of action; sensing an intrusion, making sense of that intrusion, making a decision on how to block it and taking action to implement that decision. While Fonash acknowledged concerns in terms of unintended consequences of the automation, he noted those concerns could be overcome through a better understanding of automation and its consequences and implementing mechanisms to allow for a quick reversal of automated actions. Trust among participants in the cyber ecosystem is critical for information sharing. To build trust, Fonash said, partnerships with the Information Sharing and Analysis Centers (ISACs), and now Information Sharing and Analysis Organizations (ISAOs), are facilitating the organized sharing of best practices. Another critical piece for information sharing is an infrastructure that supports resilient communications. Fonash noted the infrastructure is currently transitioning from a circuit-switch technology to an IP-based technology. Also, DHS uses a motto of "see something, say something" to facilitate information sharing; if you see something with regard to cybersecurity, report it to the rest of the ecosystem so action can be taken to patch the vulnerability and potentially avoid attack. Fonash said the government will facilitate these ideas and actions, but the desire is to have industry lead.

Discussion during the question and answer period focused on financial and nonfinancial incentives that might motivate the private sector to innovate and collaborate, the international component of what DHS is doing to help foster standards and how to mitigate some of the risk across multiple industries related to the growth of the Internet of Things. Fonash pointed out part of the problem in any discussion about security is the threat is always changing and that fraudsters are better and quicker right now than the industry—a cottage security industry versus an automated adversary. He suggested that government will influence adoption by bearing the cost of developing and setting specifications and then making them part of the contracting process for both DHS and the Department of Defense. Data standards, he said, are a necessary component of working with other countries, adding that the United States does partner with other countries in these efforts. Fonash said it would be more desirable to have security built in to devices rather than added on to mitigate risks, adding he can see Internet service providers offering services covering all of a consumer's devices, such as smart refrigerators and dishwashers.

VII. Managing the Threats to Data Security

The session “Managing the Threats to Data Security” addressed how—even with various security standards, protocols and procedures in place—breaches and vulnerabilities have progressed. During a panel moderated by Tracy Kitten of Information Security Group, Mark Carney of FireMon, Robert Carr of Heartland Payments Systems, Liz Garner of the Merchant Advisory Group and Vernon Marshall of American Express discussed what the payments industry needs to do to enhance data security and why it is not already taking more action.

Among the standards discussed were the Payment Card Industry Data Security Standards (PCI DSS). The panel agreed that though there is a need for a risk-based, consultative approach to compliance with these standards, the natural tendency is a check-list mentality. So, instead of being gray, the assessment process is black and white. Carr observed that PCI compliance is assessed at a moment in time; however, if a breach occurs, the implication is that the merchant or processor was no longer in compliance. Carney noted that entities have different challenges with compliance. For large merchants, it is about scope and/or scale, while for smaller merchants the problem is lack of knowledge and resources to respond. Carney added

that the range of emerging payments technologies has security implications that should be considered, and that present challenges for the standards body to keep up with. Garner advocated for open standards to help promote incentives to comply with PCI. Panelists suggested that without a centralized platform to protect against breaches, compliance with PCI DSS is a confusing process at best.

The conversation then shifted from requirements designed to ensure secure processing, storage and transmission of payments data within and across organizations to the U.S. migration to EMV chip and signature standards, which target securing the point of sale (POS). Carr discussed the investment his company made years ago to develop a POS encryption technology that enables encryption that protects card data from the point of capture throughout the transaction to the point at which the data are decrypted. He asserted that even if stolen, criminals cannot use the encrypted data to create counterfeit cards or make fraudulent CNP transactions, as long as the keys to decrypt the data are not stolen. Garner cited statistics suggesting that merchants bear 38 percent of fraud, issuers bear 60 percent and consumers bear 2 percent; however, absent from that equation are the networks that developed the EMV technology, who bear no cost if the technology fails to become adopted or provides inadequate security. Further, the majority of the panel indicated the most secure option would include PIN authentication instead of signature and questioned why networks are not promoting that option. Marshall said PIN presently is not widely deployed at merchant locations. He said there was a desire to ensure the most consistent customer experience. Customer service is paramount and security is an aspect of customer experience. So, the decision was made to deploy chip and signature, which provides roughly 80 percent of the benefit. However, Marshall noted that preparations are under way at American Express for chip and PIN.

From the POS, the conversation shifted to discussion about CNP transactions, for which fraud is anticipated to increase as a result of the migration to EMV. CNP fraud is costly and, according to Garner, merchants bear 74 percent of that fraud. Garner said in the online environment, the lack of multifactor authentication on payment cards is the culprit. For merchants, it is a difficult investment decision, and for issuers, there is a possibility they may lose top-of-wallet status. Still, doing the right thing for security suggests the need for multifactor authentication.

Questions about the role of the Federal Reserve generated some lively discussion among panelists and participants. Marshall noted one obvious contribution the Fed could make would be to do the same type of fraud-loss reporting as in France and the United Kingdom. Kitten observed that discussions in years past made it clear the Fed did not want a hands-on role in overseeing the migration to EMV and that it should fall to the private sector. Garner praised the efforts of the Fed's current task force to bring stakeholders together to discuss a number of security issues.⁴ Carr added that having the Fed, as the most respected institution in the ecosystem, recommend best practices would be better than what is in place now. Another question centered on the fact that although the industry has spent billions on fraud prevention, fraudsters are still out-innovating the industry; asking is it time to forget about protecting the system and figure out how to do clean transactions in a dirty system? Marshall suggested solving the problem by first protecting the data and also protecting usage. Carr referred to a remark from Powell's keynote, that "Preventative measures are not adequate" and do nothing to guard against a host of potential threats from within—employees. As the panel concluded, there was agreement that while each deployment of enhanced security standards chips away at the larger issue, no one security standard or application is the "silver bullet." Instead, a multipronged security approach—EMV, encryption and tokenization—is needed.

VIII. Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?

The session "Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?" built upon sentiments shared in the previous session, examining ways in which payments data can be devalued. During a panel moderated by Marianne Crowe of the Federal Reserve Bank of Boston, panelists representing network, issuer, processor and standards committee perspectives discussed how tools such as tokenization and end-to-end encryption can be used to enhance payments security.

As the dialog began, Steve Schmalz of RSA, The Security Division of EMC, urged that a first order of business was clarification of what "tokenization" entails and suggested that the notion of it as a "magic door" needs to be dispelled. He noted there are pre-authorization tokens, which can be used to initiate the transaction, and post-authorization tokens that act as

a pointer that allows for retrieval of the primary account number (PAN) when it is needed. Each type of token has a different risk profile.

Radha Suvarna of Citibank remarked that EMV, tokenization and point-to-point encryption together provide an opportunity to drive better value and enhance the security of the payment ecosystem. None of these by itself is the silver bullet. But together, they begin to deliver a better, more secure solution for consumers by making the transaction information less useful. Suvarna said tokenization allows the context in which the payment is being used to become a determining factor in whether to accept or decline a transaction. Madu Vasu of Visa shared how tokens for mobile payments, such as those offered by Apple and Google, are created and provisioned onto a mobile application. Both Suvarna and Vasu agreed that tokenization coupled with EMV cards makes payment transactions more secure by devaluing the underlying data. So even if the token is compromised and used in a CNP transaction, it would not get authorized.

Branden Williams of First Data Corp. noted that tokenization has turned into this year's version of big data, the cloud or virtualization, where people do not necessarily know what it means or, perhaps more importantly, what it means to them. He said that aside from trying to reduce PCI scope by deploying technologies like tokenization, the industry is marching along to the beat of the PCI drum, and nobody has stopped to ask why, whether it really makes sense, or if the problems that we need to be solving are actually being solved.

On the matter of encryption, Schmalz suggested use of the term “cryptographic mechanism” because a lot can be done with cryptography other than just encrypting something; for example, a digital signature can be created. Schmalz noted that a digital signature enables not only confidentiality, but also protects the value of a transaction and its integrity. Further, it facilitates repudiation, and ensures that information cannot be changed; in essence it locks information in so a certain piece of the information can only be used in a certain way. Vasu added that a hybrid solution based on needs is very important. As an example she noted a combination of encryption with tokenization with the payment account reference (PAR) is important for merchants.⁵ The PAR basically gives the ability to tie the payment credential across multiple token requesters.

The discussion progressed to security issues associated with storing

tokens. Vasu offered that from a network perspective, the pre-authorization token is protected in a highly secure zone and the provider is the only one who has the ability to detokenize. Schmalz noted the ANSI ASC X9 F6 tokenization standard addresses how to secure what is called the tokenization service, which includes that vault, and addresses how to secure authentication and authorization, the ability to ask for a token or detokenization services, etc.⁶

With mobile, provisioning of the pre-authorization token depends on the provider: secure element on the device or host card emulation (HCE) in the cloud. Vasu acknowledged there are some security concerns with HCE; but those have been addressed with a limited use key that is dynamic in nature, and has certain parameters or thresholds like the number of transactions, the transaction amount and the usage. Suvarna added that there is a need for a ubiquitous solution that drives consistency and provides volume, but regardless of whether secure element or HCE, mobile transactions made with a token are more secure than those without.

For CNP and e-commerce transactions, panelists agreed that pre-authorization tokens are applicable. B. Williams observed that tokens whose standards were developed by EMVCo are utilized by Apple Pay and there is an opportunity for companies that have mobile apps to follow suit. However, he also noted that whether tokens actually solve the CNP problem warrants examination. Suvarna stressed that while tokenization is a great technology, mobile apps, at best, only represent 0.01 percent of payments volume and that tokenization needs to be applied where the volumes are; where the ecosystem can more fully realize the benefits.

During the audience question and answer period, a question was posed about what can be done to devalue a card number and its use on a computer that might have malware, and also on the merchant back-end networks. Panelists generally agreed there is little to be done to protect a consumer from using a computer that has malware. Schmalz suggested it might be possible to produce a token that detects endpoints that have malware on them and then alert the owner and/or reject transaction, but there still would have to be some form of intervention. Vasu noted there have been discussions with companies in the browser business about using tokenization but that has been described as a huge effort. B. Williams agreed the industry cannot protect the consumer who has malware, adding consumers have to participate in their own rescue.

IX. Role of Industry Collaboration in Payments System Security

In the session “Role of Industry Collaboration in Payments System Security,” industry executives—within and across sectors of the payments system—addressed how they are making a joint commitment to advance payments security through dedicating time and resources to plan, advance recommendations, communicate and educate. Moderator Jonathan Williams of Experian set the scene, saying societal good is the real driver of many of the collaborative efforts under way. There is a need to share intelligence and develop common standards and systems to protect not just individual institutions but the whole payments system, including customers. J. Williams noted there are different types of collaboration, questions about on what to collaborate and when to engage. Throughout, there is a focus on what we are trying to protect. J. Williams said the various collaborative efforts represented by the panelists offered insight into leading practices.

Charles Bretz of the Financial Services-ISAC (FS-ISAC) shared that his organization was formed by the financial services industry to protect the sector from cyberattacks. FS-ISAC processes thousands of threat indicators a month—sometimes thousands a day—and has grown rapidly with 5,900 participating institutions, about 2,500 of which are financial institutions bound by its operating rules, nondisclosure agreements and under contract to share information. Bretz noted that in recognition that threats extend beyond U.S. borders, FS-ISAC has expanded to include members in Western Europe, Australia, Singapore and Japan. Membership in South America also is anticipated.

Representing the Payments Security Task Force (PSTF), Nancy O’Malley spoke about work to secure card-present transactions. The PSTF is an initiative launched by MasterCard in response to concern about the progress being made toward the migration of EMV in the U.S. marketplace. The PSTF was convened to foster a different level of collaboration at the most senior level of the payments security marketplace with the goal of gaining and securing commitment to advancing solutions purely in the safety and security space.

Sandra Kennedy of the Merchant Financial Services Cybersecurity Partnership shared the organization was formed out of a need for retailers to collaborate on a plan to address security incidents. As a first step, the Retail

Industry Leaders Association (RILA) reached out to the Financial Services Roundtable (FSR). Kennedy noted that after finding common ground on many issues, the groups decided to focus on those and move forward collectively. RILA and FSR pulled together 19 associations representing the merchant and financial services industries to focus on five key areas. Through this partnership, RILA learned much from the financial institutions involved as well as FS-ISAC and other organizations. Kennedy said that with the assistance, knowledge and experiences of these other associations, RILA was able to establish a Retail Cyber Intelligence Sharing Center, which will house the retail ISAC. She noted that, now almost a year old, the sharing center has forged a formal relationship with the FS-ISAC that will be a long-term benefit to both sectors.

Liz Votaw of the Fast IDentity Online (FIDO) Alliance observed that the FIDO Alliance is a little bit different from some of the other collaborations, but there also are similarities. What makes FIDO different is that it is not a payment-specific collaboration. It is a cross section of every type of company involved in authentication; its focus is on helping companies throughout the authentication ecosystem ensure that their implementations of authentication technology are safe and secure not only for the companies but also for their customers. Votaw said the Alliance has led to the development of a set of specifications that industries can leverage to rid themselves of reliance on passwords for authentication.

J. Williams asked how the effectiveness of these collaborations can be measured. Panelists agreed that it varies. Bretz offered that objectively, there are many metrics and the more statistics that can be collected the better. However, metrics present a challenge in that reliable statistics are rare. O'Malley and Kennedy suggested that success also can be measured subjectively, by sustained commitment to partnerships and networks that are built, which historically has not been the norm in the payments ecosystem. Votaw added that adoption of practices and specifications offers another objective measure of success.

As for challenges to collaborations, O'Malley identified overlapping initiatives of many well-intentioned groups trying to solve the same problem. She said categorizing the problem being addressed, looking at the mission and choosing carefully can help determine how best to allocate resources. Another challenge experienced by each panelist was trust. Bretz said it took 14 years for FS-ISAC to build up trust, but he has seen dramatic results

when attacked organizations shared information about an attack and asked for help from colleagues in FS-ISAC or other partner organizations. Kennedy said the industry has a shared customer, but also a shared enemy; so the more trust among its various participants, the better. She added that given what is at stake, the industry prefers to address security issues through collaboration rather than to have legislative interventions.

During the audience discussion, panelists were asked to look ahead, about three years after the implementation of EMV. Questions posed centered on where fraudsters will go after the payments system has been secured and what the focus of private sector collaboration will be. Panelists generally agreed that the industry and technology likely will have changed greatly in three years, perhaps in unimaginable ways. Votaw said she thinks FIDO will still exist in three years, focusing on the same issues. Bretz added that as the industry changes in that time, so will the criminal element, and the payments industry likely will be responding to their innovations. And, if one assumes the payments system has been secured, Votaw said the fraud next would go to where there are weaknesses in the system. O'Malley added the most immediate attack will be on CNP transactions and that current and future targets will be in nontraditional spaces not necessarily thought about from a payments security perspective but that will affect the industry. Kennedy said it is important to be constantly evolving, looking at where fraudsters are going and protecting customers.

X. Role of Government in Payments System Security

In the conference's final session, "Role of Government in Payments System Security," Gordon Werkema of the Federal Reserve Bank of Chicago guided a discussion among U.S. and international public authorities involved in policy initiatives related to deterring payment fraud and/or improving cybersecurity. During the discussion, panelists spoke about the role of government in promoting payments system security and protecting sensitive data and offered insights about the tools that regulatory bodies have at their disposal—moral suasion, regulation, operation and cooperation.

Chrissanthos Tsiliberdis of the European Central Bank (ECB) said the main objective of the ECB is to ensure that the financial market infrastructures (FMIs) are safe and efficient. To accomplish this objective, central banks and other regulators have a threefold task: to keep processes flexible enough to accommodate the pace of innovation, to ensure fair competition

among participants and to require that adequate minimum security requirements are being implemented by service providers. Tsiliberdis shared that the ECB has been actively monitoring the payments market and its initiatives to observe how participants are sustaining the efficiency and safety of the payments systems they provide to the market. He noted that over time, the ECB has observed that monitoring, in some cases, has not been successful. In response, the Eurosystem created SecuRe Pay as a forum to address issues pertaining to the security of online card payments. He mentioned that SecuRe Pay is developing new policies for the cyberresilience of FMIs and retail payments services, cooperating with other banking authorities and will be analyzing and monitoring incidents and fraud reporting. Further, Tsiliberdis shared SecuRe Pay has sanctions authority to deter cyberattacks and formulates/coordinates on legislation on cybersecurity.

Coen Voormeulen of the De Nederlandsche Bank provided insights as chair of the Bank for International Settlements' Working Group on Cyber Resilience, which is comprised of about 20 countries. The working group focuses on systemic risk and cyberresilience of FMIs and publishes guidance for overseers on how to look at FMIs in terms of business continuity, operational risk, legal risk, business risks—risk management in general. Voormeulen noted that while the guidance is for FMIs, it may be applicable in some fashion to systemically important and prominently important payment systems. Voormeulen added that cyber goes much further than information technology. It is very important that the people in an organization have a clear picture of what they need to do to protect the organization against cybercriminals. It is important to consider the whole cyberresilience profile of an organization when new services, products or tools are launched. It is important to have a communication plan in place in the event of a crisis. Finally, it is critical to have a business resumption plan for how to resume operations in a safe way, including a recovery time objective. He shared that the work group planned to publish a guidance note in November, to be followed by a two-month public consultation period—for which the world was invited to respond. The Working Group on Cyber Resilience's goal is to publish the guidance note in the spring of 2016.

Anjan Mukherjee of the U.S. Department of the Treasury noted that the payments system as he thinks of it was initially built for connectivity, not for security. Much of the architecture that underlies the payments system is legacy in nature and subject to the rapid technological change. Mukherjee

said Treasury is focused on areas of greatest risk, and given rapid accelerations in Internet use there is a need to be extraordinarily cautious. Toward that end, he said Treasury helped formulate and coordinate the Obama administration's legislative proposals in cybersecurity, which, among other things, looked to facilitate information sharing and data breach notification. He also said Treasury will use its sanctions authority to deter targeted, malicious cyberattacks.

During discussion among the panelists, the point was made that while cyberattacks have no borders, global coordination remains a challenge. Tsiliberdis observed that the optimal way to collaborate varies by country. In some countries, regulators may need to push for collaboration while in others regulatory activity may hinder collaboration. Mukherjee offered that collaboration may be stimulated in many ways, for example FS-ISAC and crisis management exercises. He noted that the biggest struggle is how to implement internationally and suggested that guidance on baseline protections and best practices, information sharing and recovery planning from the National Institute of Standards and Technology may be a useful resource for collaboration. It is a tool that can help bridge differences in cultures—in how issues of payments security are dealt with. Voormeulen added that promotion of cross-border information sharing among FMI's also would be beneficial.

Questions posed by participants to the panel included: What role do you think public authorities play in influencing culture? What is the federal government doing to help encourage various state government entities to follow the federal government's efforts? What role, if any, do public authorities have in supporting or engaging private sector-led initiatives? Voormeulen and Mukherjee agreed it is difficult for public bodies to impose culture, and that at best it is possible to bring parties together and make them aware by sharing information on best practices. Tsiliberdis added that building trust among different participants is a point of emphasis. As for attempts to persuade states to follow the federal government's lead, Mukherjee said that impediments to the federal government's ability to impose standards mean it mostly can help by facilitating discussion and encouraging membership in FS-ISAC. Tsiliberdis added that in supporting private sector efforts, "we always take under consideration what has been developed by the market and will not try to reinvent the wheel."

XI. Closing Remarks: Views from the Kansas City Federal Reserve Bank

Closing remarks were made by Esther L. George, president of the Federal Reserve Bank of Kansas City. George noted that although the Federal Reserve is relatively unique among central banks as an operator of retail payment systems, international public authorities that do not operate retail payment systems have become more active in raising concerns about their security. Some play an explicit role with public mandates while some induce voluntary action. The Federal Reserve has chosen to lead through a collaborative approach, which is not new for the Fed. George reflected that since the founding of the Federal Reserve, observers have looked to it to provide leadership on advancing safety, efficiency and accessibility of the U.S. payments system. Congress initially designed the Fed to serve as a payments system operator through the regional Reserve Banks and as an overseer of the system through its supervision of financial institutions. She said these roles give the Federal Reserve relevant insights as it works with others to address the security challenges of today.

George said that as the Federal Reserve seeks to drive improvement in payments systems through a collaborative approach, two task forces comprised of diverse and committed membership have been convened. One, the Faster Payments Task Force, is focusing on identifying and evaluating approaches for implementing a safe, ubiquitous and faster payments capability in the United States. The other, the Secure Payments Task Force, is providing input on security aspects of a faster payments capability and serves as a forum to advise the Federal Reserve on how to address security matters and to identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System.

In concluding, George said she sensed a greater degree of consensus around the security challenges the payments system faces, and noted the challenges are also opportunities to achieve a faster, more secure and widely available payments system in a way that maintains the public's confidence.

XII. Conclusion

Securing the payments system is a matter of utmost importance to payments participants and policymakers. Over the course of this day and half long conference, there was a robust exchange of thoughts and insights about

the need for data collection in standardized forms to better understand rates, prevalence and origination of fraud and security breaches, as well as the costs and benefits of various security strategies. There also was a stated recognition that there is no “one-size-fits-all” solution for securing payments systems; rather a multipronged approach is needed to improve payments security. Technologies such as encryption and tokenization do not compete; they are complementary. Coupled with these technologies that enhance data security or devalue data, stronger payer authentication can be expected to improve payments security. There also was much discussion about collaborative efforts under way in the private and public sectors, both domestic and international, to address payments security. Since payments security is everyone’s concern, deciding between private and public efforts is likely a false dichotomy; instead, the private and public sectors need to work in tandem. These insights will help inform the decision making of central banks, other policymakers, and private sector payment participants as they approach solving the puzzle of payments security.

Endnotes

¹<http://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

²The Observatory, created in November 2001, is a forum for fostering dialogue and information sharing among all parties in France concerned with the smooth operation and security of card payment schemes. The APCA is a self-regulatory body set up by the payments industry to improve the safety, reliability, equity, convenience and efficiency of the Australian payments system. APCA's 100 members include leading financial institutions, major retailers and other principal payments service providers.

³3D Secure is a technology for authenticating the payer of an online purchase, and requires adoption by the online merchant, the acquirer and the card issuer.

⁴The Federal Reserve System's Secure Payments Task Force was convened to engage a diverse array of stakeholders in advancing the work outlined in "Strategies for Improving the U.S. Payment System," published in January 2015. The mission of the Secure Payments Task Force is to provide a forum for stakeholders to advise the Federal Reserve in its leader/catalyst and operator roles on payment security matters, and identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System.

⁵The payment account reference facilitates receipt of the PAN for loyalty programs and for fraud and risk. If this information is sent in the clear it defeats the purpose of tokenization.

⁶The American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X9 F6 work group is working on a security tokenization standard that addresses tokens used after initial payment authorization (i.e., post-authorization tokens), such as when an acquirer provides tokenization services to merchants.

Opening Remarks



Kelly J. Dubbert

Good morning and welcome to Kansas City. We are pleased to have you join us for this, our fifth international payments conference, “The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System.” The focus of this conference is intended to recognize the many participants, technologies and issues involved in securing the retail payments system. This has never been simple and has only become more complex given the pace of growth and innovation within the payments system.

The flow of goods and services relies on a well-functioning payments system, and security has always been a key component of those transactions, which are a critical part of the economy. Central banks, for their part, also have an important role in assuring public confidence in the system.

The past few years have been fraught with one high-profile security incident after another that have revealed shortfalls not only in our ability to prevent attacks, but also to effectively detect and respond to them in a timely manner. With each new announcement of a security flaw within a payments network, at a retailer or at a bank, public confidence in the safety and security of the retail payments system is shaken. Security compromises in retail payment systems are not new. We have experienced and managed risks as payment methods have evolved, including with check processing and ACH. However, as payments have become increasingly electronic—at the point of sale, at ATMs, online and mobile—and as the payments infrastructure evolves to make payments even faster, the risks have inevitably grown and become more widespread. So while risks in the past were managed with changes to processes and rules that were focused primarily on how financial institutions accessed the payments system, today there are millions of endpoints made up of merchants, providers and innovators that need to be included in the security “conversation.”

That conversation—which requires the active engagement of the spectrum of payments system participants—is one of the goals for this conference. As the central bank for the United States, and as both an operator and an overseer of the financial institutions that many use to access the payments system, the Federal Reserve is in a unique position to promote the involvement of the respective industry segments.

Certainly there are practices and experiences that are beneficial to us all. So, we have organized our agenda to first delve into the current landscape and then to examine how private and public policies can address the significant security issues we must face together.

We will begin this morning by outlining the roles participants need to play to build a more secure payments system. Each of us—financial institutions, operators, networks, processors, merchants, innovators, businesses, consumers and regulators—has a role to play. Hearing the charge, we can begin to learn how economic analysis can help us to better understand and overcome one of the biggest challenges we face—coordination problems. We need a better grasp of why some coordination efforts succeed while others fail. With such an understanding we then can promote a convergence toward long-term solutions that could benefit the entire system, rather than solutions that only meet immediate needs.

The discussion will turn to another key challenge to addressing payments security: the ability to collect or obtain data on payments fraud, data breaches and other indicators of weak security that are necessary to properly distribute our resources to appropriate security defenses. That challenge is being met in various places in the payments system, and this information is influencing and motivating action where it is available. This conversation can help to spur thinking about how we might be able to solve some of the difficulties in gathering the data needed to drive broader improvements.

We will then hear from a range of stakeholders on the front lines of dealing with threats to data security, which is core to retail payments security. They will share how available resources factor into their ability to effectively prepare, prevent and manage threats and discuss ways to go a step further, to devalue payments data, or make it worthless to those who continuously attack our systems to obtain it.

So how do we work together to get all of this done? On Friday, the discussion will center on how the private sector is collaborating to improve security

for payments transactions from initiation to receipt, within payment networks and, from a critical perspective, across the entire payments system. That will be followed by a dialogue about the role of government in promoting payments system security and protecting sensitive data—when, how and why is government engagement or intervention appropriate in addressing security questions?

As you can see, there is much that we hope to accomplish in this day and a half. The presentations are meant to be a starting point; to set the table for what is to come. The puzzle of payments security we face today cannot be solved by working separately. This conference is an opportunity to consider how the solutions we have discovered can be leveraged collectively to address the system's broader challenges.

With that, I would like to introduce this morning's keynote speaker, Governor Jerome H. Powell. I will let you reflect on his bio, which is included in the program, but will highlight a few key points: Governor Powell was confirmed by the U.S. Senate to the Federal Reserve Board of Governors in 2012 and then again in 2014. Before joining the Federal Reserve, he was a visiting scholar at the Bipartisan Policy Center in Washington, D.C., and he previously served as an assistant secretary and undersecretary of the U.S. Treasury Department, where he had responsibility for policy on financial institutions, the Treasury debt market and related areas.

Earlier this year, he became co-chair of the Federal Reserve's Payments Improvement Initiative, which is a multifaceted effort for collaborating with businesses, emerging payments firms, card networks, payments processors and financial institutions to enhance the speed, safety and efficiency of the U.S. payments system. This is an important effort you will be hearing much more about over the next two days. Please join me in welcoming Governor Powell.



Building a Safer Payment System Through Collective Action

Opening Keynote

Jerome H. Powell

Thank you for the opportunity to speak to you today. I especially want to thank Federal Reserve Bank of Kansas City President Esther George for her leadership in the initiative that has brought us all together here today to discuss improvements to the U.S. payments system. We have a diverse group of professionals participating in this conference, from industry, academia and government. It takes all of us, working together, to maintain and enhance a safe and secure payment system.

The payment system touches our daily lives, whether it is a consumer paying a bill, a company deciding to upgrade its point-of-sale terminals, a technology startup developing a new peer-to-peer payment app, or the government issuing tax refunds. Americans make more than 120 billion noncash payments each year.¹ But it is only when something goes wrong, like a data breach at a major retailer or bank, that the typical end-user takes notice of the payments process.

As the central bank of the United States, the Federal Reserve plays many roles in the payment system, including payment system operator, supervisor of financial institutions and systemically important financial market utilities, regulator, researcher and catalyst for improvement. Most of you are aware of our current efforts to improve the speed, efficiency and security of our payment system. I would like to discuss that project for a few minutes, and then talk about four things that we should all be doing to enhance payment security.

For some years, members of the public have told us with increasing frequency and intensity that they see the United States falling behind other nations in the speed and security of our payment system. We hear all the time that the Federal Reserve should do something about this. But, despite our multiple roles, the Federal Reserve does not have broad authority

to simply restructure or redesign the payment system. So, two years ago, the Fed published a consultation paper that sought public input on ways to make the U.S. payment system safer, more accessible, faster and more efficient from end to end.² As we evaluated the substantial volume of public comment in response to the paper, the Fed also conducted research; met with a wide set of stakeholders, including banks, merchants, technology companies, consumer organizations and others; and worked to enhance our own payment services.

Building on this work, we released a second paper earlier this year, titled “Strategies for Improving the U.S. Payment System.”³ This paper synthesizes a range of views and presents a multifaceted plan for collaborating with payment system stakeholders to enhance the speed, safety and efficiency of the U.S. payment system. The paper emphasizes the need for a secure payment system that has the public’s confidence and that keeps pace with the rapidly evolving and expanding threat environment.

To facilitate cooperation among the many stakeholders, under the leadership of Esther George, we have established two task forces: one for faster payments and one for payment security. These task forces will work both independently and in concert. The security experts on the Secure Payments Task Force will advise members of the Faster Payments Task Force as they identify effective approaches for implementing faster payment capabilities. The Secure Payments Task Force also will advise the Fed on payment security matters, and determine areas of focus and priorities for future action to advance payment system safety, security and resiliency.

I am pleased to report that we are off to a great start in the months since the “Strategies for Improving the U.S. Payment System” paper was released. More than 300 participants from a range of stakeholders signed up to be part of the Faster Payments Task Force, and more than 200 joined the Secure Payments Task Force. These task forces have chosen, or are in the process of choosing, members to serve on their respective steering committees, which will help guide the task forces’ efforts.

Earlier this month, the Faster Payments Steering Committee met to begin developing timelines, processes and criteria—including criteria related to security—that will be used to evaluate potential approaches to improving the speed of the payment system. Last week, the full task force met to continue the work. I am told that they had a great meeting—everyone was interested,

engaged and eager to get to work. The Secure Payments Task Force conducted its first organizing call earlier this month and, in mid-July, its steering committee will meet for the first time. Momentum is growing. By the end of next year, the plan is for the Faster Payments Task Force, with input from the Secure Payments Task Force, to have laid out its detailed thinking on the most effective approaches for implementing faster payments in the United States. Then, it will be up to the industry to implement these approaches.

But, before we reach the finish line, the task forces will have to wrestle with some tough issues related to payment security. I would now like to talk about building a safer payment system. I will start with two brief stories.

First, let me take you back to the 1960s, when paper checks were the dominant noncash payment method and were sent by plane or truck to be cleared. A man walks into a bank with a payroll check. A teller cashes the check. A few days later, the man returns. The teller recognizes him, and is happy to cash more checks. The checks are fraudulent, but the teller does not know that. The man knows that the string of numbers encoded on the bottom of the check determine the geographic area where the check will be drawn. So he creates a fake check with a routing number that will send that paper check across the country. Because the teller recognizes the man when he comes back, the teller feels comfortable cashing the second round of checks because the first check has not yet been returned. By the time the bank realizes the checks are fraudulent, the man is gone. Some of you will recognize that man as Frank Abagnale, former con artist and now a security consultant.

Now, fast-forward 50 years to 2013. A man walks up to an ATM with a prepaid debit card. He types in a PIN and withdraws a large amount of cash. But it is not just one man: there are many individuals doing the same thing at thousands of ATMs in dozens of countries. The cards are counterfeit, but no one has detected that yet. Over the course of 10 hours, the individuals withdraw \$40 million in cash. How does this happen? Before the thieves walk up to the ATMs, hackers break into a payment processor's database, steal a small number of prepaid card account numbers and raise the cards' withdrawal limits. They then distribute counterfeit cards to "cashing crews" around the world who make the withdrawals.

These well-known payment fraud schemes were perpetrated in different eras, and juxtaposing them highlights how the payment security landscape has changed. Frank Abagnale relied on the slow speed of the paper check-clearing system and in-person social engineering. In contrast, the

ATM thieves relied on rapid transmission of data to remotely steal account information and alter withdrawal limits, all without interacting with bank employees. Today, fraud can be executed quickly, perpetrated on a massive scale and carried out remotely.

In light of this new environment, I will suggest four things that all of us ought to be doing with respect to payment security. Some are already being done. Too often, though, such efforts are overlooked or inconsistently applied.

I. Safe innovation

This is an exciting time for the payment system. Technology companies are creating new methods to pay with mobile phones and even wearable devices. Banks are building faster payment capabilities into their deposit account systems. Banks, payment card networks and merchants are rolling out Europay, MasterCard and Visa (EMV) chip cards and using compatible point-of-sale terminals. Many of the newest products in the market are impressive, incorporating new technologies like biometrics and tokenization. End-users and the media have taken notice.

History shows that we should embrace innovation. Technological innovation has continually pushed the payment system forward. Payment cards, both credit and debit, are an example. Thirty years ago, everyone carried cash. Today, young adults increasingly prefer to rely on cards and mobile phones. Payment cards have improved convenience and security in certain ways, like reducing the impact of a stolen wallet.

But history has also shown that new technologies must be adopted in a prudent fashion. Technological innovations can provide substantial benefits to payment system efficiency and security in the long run, but they often introduce new, unanticipated risks. For example, although payments cards reduced the impact of a stolen wallet, they have also introduced new risks, like counterfeit card fraud. It is important that we identify and address the unanticipated risks that inevitably result when we try new things. These risks may be tolerable in the short run, so long as we work to identify, prevent and mitigate them early on in the design and implementation process. In the case of payment cards, over time, technologies have been broadly implemented to mitigate many of the risks. For instance, computer algorithms now analyze transactions in real time and can prevent the same card number from being used to make purchases in Washington, D.C., and in Kansas City five minutes apart.

We also need to consider the complexity of the payment system. It is a vast network with millions of endpoints and a wide variety of participants. Many innovators do a good job of incorporating advanced security features into their individual products. But new products also need to be securely integrated into the payment system as a whole.

To innovate safely, payment system participants must work together by participating in coordinated efforts to improve the payment system. At a minimum, banks, merchants and other institutions that process or store sensitive financial information need to keep their hardware and software current to the latest industry standards. Network operators and standards-setting bodies play an important role by identifying these standards and coordinating their adoption among network participants. The EMV rollout that is taking place right now is a good example.

The market should be the primary driver of change, and government should avoid stifling healthy innovation. But policymakers can play a role by actively listening to concerns from the public regarding barriers or gaps in regulatory regimes that may create disincentives for developing new, safe products. Policymakers can also bring industry participants together. The task forces that were created as part of the Fed's payment system improvement effort bring together a wide range of payment system participants to sit at the drafting table to create a blueprint for a safer and more efficient payment system.

Complacency is everyone's enemy. Unfortunately, the firms involved in the payment system are not the only ones innovating: criminals have an ever-increasing arsenal of cyberweapons at their disposal. That brings me to my second point.

II. Prevention

You *will* be attacked. Criminals today are often motivated, intelligent, well-organized and well-funded. They also have varied interests: some seek financial gain, while others hope to disrupt our nation's financial institutions and payment system. What should we be doing to prepare? One clear area of focus needs to be on implementing preventive tools, or simply put, defensive tactics. You will not survive the game if you do not play good defense.

The deployment of EMV chip cards in the United States represents an important step forward. But we should not stop there. For many years,

traditional authentication methods like signatures and static passwords have been used to verify that an individual is authorized to initiate a payment. New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions.

It is important to layer security tools and procedures. Methods to devalue payment data, like tokenization and encryption for data at rest, in use and in transit, mitigate the effect of a data breach. Analytics can identify and prevent fraudulent transactions. Firewalls and segmentation of technology supporting critical functions can protect networks from outside attacks.

Also, remember that people inside your organization and organizations that you work with can pose a significant risk. One study found that more than 20 percent of security incidents could be attributed to insiders.⁴ Segregation of duties, background checks and monitoring for anomalies help reduce the risk of insider threats. Strong vendor-management programs can reduce risks from an institution's partners and service providers.

III. Planning

As crucial as they are, we should keep in mind that these prevention tools cannot stand alone. Even with stronger authentication methods, robust network security and other approaches in place, preventive measures are not sufficient to manage security risks. Such measures are designed to protect against known risks. But those looking to exploit the system will continue to devise new methods of attack. In some of the recent high-profile data breaches, companies have scrambled to deal with the aftermath. This brings me to my third point. We need a comprehensive way to think about planning. The National Institute of Standards and Technology's (NIST) cybersecurity framework is one of many voluntary cybersecurity frameworks that provide a holistic, risk-based approach to planning.⁵ In addition to preventive measures, the framework identifies four additional core functions: identify, detect, respond and recover. We can apply these four functions to securing the payment system.

An important first step is to identify internal business processes and assets, as well as external threats. You cannot protect yourself unless you understand how your business is structured. This sounds simple enough, but an organization's computer systems are often unexpectedly interconnected. Some of

the largest point-of-sale data breaches, for example, originate outside payment card systems.⁶ You should also keep up to date on cyberdevelopments and gather information about threats from information-sharing forums, including the Financial Services Information Sharing and Analysis Center, the U.S. Computer Emergency Readiness Team and the FBI's InfraGard.

Regardless of how well we identify and protect, we also need to plan for a potential attack. To address this, the NIST framework calls for plans to detect, respond and recover. Victims are often not aware that they have been breached. Did you know that last year the median amount of time it took to discover a breach was about 200 days?⁷ Plans need to include methods to detect attacks. You also need to have a response plan. If your point-of-sale system is compromised or your account records are stolen, do you know which law enforcement agencies you should work with? You will be more effective containing the impact if you have thought through the necessary responses beforehand. Finally, you need to have plans in place to recover business functions. This may include investments in new tools and approaches to aid in rapid recovery. I would also advise that you participate in industry-led tabletop exercises to help you think through how to respond and recover from cybersecurity events.

IV. Education

We have talked a lot about fostering the security of the payment system, but we should also talk about the public's perceptions. Even if we have a comprehensive, well-implemented security plan, one high-profile breach can shake public confidence. Research suggests that the way consumers feel about a particular payment mechanism affects the way they choose to pay. For example, the Federal Reserve's most recent report on consumers' use of mobile financial services notes that security concerns are a main impediment to the adoption of mobile financial services.⁸ Education is a way to enhance both payment system security and public confidence.

My fourth point is that, collectively, we could do more to empower consumers to use financial products safely by educating them on the risks they face and the steps they can take to protect themselves. For example, financial institutions can provide and help customers understand online banking tools like credit card transaction alerts that can help consumers spot or stop fraud. We also need to be prepared, to the extent possible, to respond to a security incident in a transparent and timely manner so

consumers understand the implications of the event. Policymakers can also provide facts and data to paint a realistic picture of the threats that exist in the payment system. One example is the Federal Reserve's triennial payments study, which presents statistics on fraud for the largest retail payment systems that could be used by companies and the media when explaining risks to consumers.⁹

Knowledge is power. Education is critical to fostering the security of the payment system and, ultimately, to maintaining public confidence.

V. Conclusion

The things I have discussed today apply to all payment system participants. Each of us has an important role to play in building a safer payment system. Given the payment system's complexity, it is important to keep in mind that we all need to work together when we innovate, prevent, plan and educate.

I want to close by asking for your support. With our payment system improvement effort in full swing, now is the perfect time for payment system participants to come together to build a safer and more efficient payment system. If you have joined one of our task forces, I hope that you will maintain a high level of engagement. If you have not, I encourage you to do so, or at least to follow their progress. We will continue to seek input and provide updates through live and virtual forums, surveys, industry- and Federal Reserve-sponsored groups and events and online feedback mechanisms. Thank you to the Federal Reserve Bank of Kansas City for organizing this conference and to all of you for participating.

Endnotes

¹Federal Reserve System (2013), “The 2013 Federal Reserve Payments Study: Summary Report and Initial Data Release.”

²See Federal Reserve Banks (2013), “Payment System Improvement—Public Consultation Paper.”

³See Federal Reserve System (2015), “Strategies for Improving the U.S. Payment System.”

⁴Verizon (2015), “2015 Data Breach Investigations Report,” www.verizonenterprise.com/DBIR/2015.

⁵See National Institute of Standards and Technology (2014), “Framework for Improving Critical Infrastructure Cybersecurity.”

⁶Verizon (2015), “2015 Data Breach Investigations Report,” www.verizonenterprise.com/DBIR/2015.

⁷Mandiant (2014), “M-Trends 2015: A View from the Front Lines,” <http://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf>.

⁸Board of Governors of the Federal Reserve System (2015), “Consumers and Mobile Financial Services 2015.”

⁹See Federal Reserve System (2014), “The 2013 Federal Reserve Payments Study: Detailed Report and Updated Data Release.”

General Discussion

Building a Safer Payment System Through Collective Action

Mr. Dubbert: Very good, we will open it up for questions from the audience. Let me start. Governor Powell, obviously, all of us have heard a great deal about the Office of Personnel Management (OPM) breach in recent days and weeks. If you might reflect on that, the scale of that breach, and its impact on the federal government. Is it a watershed moment perhaps in how we rally collective resources of the government and the private sector to try to move forward to address the underlying issues there?

Mr. Powell: I will say that it seems to me to be a very important event and something that we are living with daily. I have a great portion of the administrative responsibilities that the governors share on the Federal Reserve Board. So I will just say that we are very focused now on understanding what happened. We are still learning very much what happened over at OPM. We are focused on communicating about that to our employees. And we are focused on looking out for our employees. We are determined to look out for the best interests of our employees throughout the Federal Reserve System on this. I would just say we are living through this personally right now at the Fed, through the whole system, particularly at the Board, and living the reality that we all face.

Mr. Stervinou: You talked about basically moral suasion and the role of the Federal Reserve and the Board of Governors in driving the market toward the goal of faster payments and security. When we talk about security, there is the oversight capacity and the supervisory capacity of the Federal Reserve. Do you think that there is a need also to go further, to push the market a little bit more in the direction of more security? I mean, to use your mandate to actually drive a little bit more the security aspects of what the market players are putting in the field?

Mr. Powell: Thank you for your question. Remember what we do is we supervise banks, not all financial institutions, just banks—state member banks and all the holding companies. At our Federal Financial Institutions Examination Council, we have guidance in place and we do supervise banks. Guidance requires banks to have secure information programs and that kind of thing. So it is an area of intense focus for small, medium and large banks, and for our supervision of them. We have people who are expert in that area who really focus just on that, and it goes to both the security program and also the response program. So we are doing a great deal. I think any of our regulated entities would tell you that it is a major focus. It is also a focus for us in our own payment activities. I think it is important to say again that we do not have this plenary authority over the financial system or over the whole payment system, which I think some other countries—and I am not recommending these things—have much more consolidated financial systems than we do and have much more concentrated authority to regulate and supervise them. Our own authority is quite specific and does not extend to non-regulated entities. Now, I would also add that many entities are regulated at the state level and also regulated by other federal entities. It is not that they are completely unregulated, but they are not regulated by the central bank or by other banking regulators. And just to echo that, it is something we spend a great deal of time on as do all of the financial institutions we supervise.

Mr. Grover: When consumers and businesses are asked whether they like the idea of faster payments, they almost universally or certainly a large number say yes. Do you think, however, there is a commercial case to be made for faster payments?

Mr. Powell: So the question is whether there is sort of a commercial use case, and I think the answer is yes. I think one needs to be objective about it. We looked carefully at what the use cases were, and they exist. Consumers do want some faster payments, businesses want some faster payments; not every payment needs to be made instantaneously. So the initial use case may be fairly confined in scope. On the other hand, it is really hard to know. Once faster payments come along, it may be that adoption is very wide and there is quite a lot of adoption and support for it. But we are very mindful of where; that it is just not some broad thing where everyone needs every payment to be settled right away. That is really not the case.

Mr. Carr: Governor, I really appreciated your comment that—I wrote this down—“Preventive measures are not enough,” and your talk about insider issues. I do not really understand why there has not been a wholesale movement to encryption of data so that when we are penetrated and when our people make mistakes, we are better protected; we are coming up to the EMV period here. Oct. 1 is a big day. There are many of us putting a lot of energy and effort into rolling out EMV, and I am getting chip cards these days, and when I use my chip card on Oct. 2 and there is a breach, my PIN is still going to be exposed. I just wonder whether consumers are going to be expecting to have fewer problems with breaches because of EMV. Certainly it is going to be more difficult, impossible perhaps, to make counterfeit cards, but the data is still there to do card-not-present fraud for these chip cards. And it baffles me why we have not moved to chip and PIN with these transactions to protect them, and if we have not, why in the world are we not encrypting this data? That is an observation. I just appreciate your comments.

Mr. Powell: That is a great question and I think there are plenty of people in the room who you might address that to as the conference goes on. We do not land on any one particular thing and say we have to do this, but clearly PIN is better than signature, and there are other things that may be better than PIN, and we believe in layering. We are learning as we go and unfortunately one of the ways we learn is by making mistakes and getting breached and figuring it all out. It is one of the purposes of this conference; to try to move that dial forward.

Ms. O'Malley: I am interested, Governor Powell, in your perspective as a member of the Board of Governors on the introduction or the entrance of these new digital giants into the marketplace and the roles they are playing now in authentication and the delivery of payment services to consumers. I am sure the Board of Governors has had a lot of debate and I would be interested in your insights on this issue.

Mr. Powell: And when you say new digital giants, what are we talking about here?

Ms. O'Malley: Apple, Google, etc.

Mr. Powell: The Board of Governors does not have a position on that. It is not something we actually debate. But I think our overall position is to be supportive of innovation in the payments system. Even on Bitcoin, if you saw Chairman Bernanke's letter last year, what he said was, “Look, we

generally support innovation in payments. It is progress.” And again, as I said, what choice do we have? Innovation is ongoing. The thing is it has to be done safely and it has to be done in a way that does not enable money laundering and things like that. So that is not an issue with the companies you mentioned, but it could be with some of the virtual currencies. So I guess just speaking for myself, my broad sense is these are things the consumers want, the consumers are getting, and it is up to those of us in the supervision, regulation, public communication spheres to make sure that the way they get them is well understood by the public and well regulated and supervised by the government so when problems happen, we have anticipated them and done what it is we can do.

Mr. Horwedel: Earlier you spoke about other markets in which there was some sort of government mandate to move payments forward. Given all the inertia in the U.S. payments market, do you really think that it is possible through trying to build consensus that we can draw even with or surpass other markets that are now considerably more advanced than we are in payments?

Mr. Powell: Actually, I do, and I will tell you why. In our system, I do not put a lot of probability on the idea that we will evolve in the direction of a more consolidated financial system or consolidated regulatory, or that we should want to. It is just assumed that it is what it is and it is not going to change, which is very likely. Look at what we have. All of these innovating companies are here. They are in the United States. They are involved, many of them, in our payment system efforts. So we also just have a more flexible economy. We have far less in the way of what economists like to call structural rigidity. So we are able to innovate. I am not saying it is going to be easy, but I actually feel like we have a chance to do something really constructive here with our payment system initiative and I am very excited about the prospects for it. I hope I am not naïve about the difficulties, but we have a lot of assets as well as other attributes.

Mr. J. Williams: Governor, the number of different payment systems that comprise the whole retail payment system is only increasing. New payment mechanisms are being invented almost daily. What do you think the role of retirements and renovation of the legacy payment systems we currently have is in actually reducing the envelope that we are trying to secure? I have to say the United States and many other European countries are not much better than we are in the U.K., but I would be interested in your view.

Mr. Powell: A really interesting question. I guess it would not be inappropriate to share when I joined the Board three-and-a-half years ago, there was an important decision being made over whether we should migrate off Lotus Notes. And we did do that with a lot of pain and suffering too. So I guess that question is probably better addressed to some of our subject matter experts here. But these legacy technologies tend to last a long time. We were talking at dinner last night with Peter Fonash. He said people are still using COBOL actively, which I remember learning about a couple years back in the ninth grade, eighth grade. So you are right, it does present a challenge. But we can push forward and embrace what we seem to be good at, which is technological innovation and flexibility. All we can do is the best we can.

Mr. Dubbert: Governor Powell, thank you very much for being with us today and for your personal leadership on behalf of the Board of Governors in the payment space.

Mr. Powell: Thanks again, and have a great conference.

The Economics of Retail Payments Security



Fumiko Hayashi, Tyler Moore and Richard J. Sullivan

I. Introduction

In recent years, weaknesses in payment security have become increasingly evident through a constant stream of news reports on data breaches, phishing attacks, spoofed websites, payment card skimming, fraudulent ATM withdrawals and online purchases, computer malware and infiltration of retail point-of-sale systems. Although these events seem not to significantly affect current end-users' payment method choices, they may hinder adoption of new technologies, such as mobile and faster payments (Schuh and Stavins). Were the public to lose confidence in the payments system, however, payment behaviors could drastically change, potentially undermining commerce and overall economic activities.

Motivated by various factors, all involved parties make continuous efforts to improve payment security. Financial institutions, payment networks, processors, businesses and consumers take steps to mitigate security threats. Regulators help to ensure compliance with appropriate security practices. Law enforcement puts pressure on attackers to deter bad behavior. However, while these continuous efforts to improve the payments system are under way, attackers are becoming more sophisticated in finding weak links and developing new modes of attack.

To better understand the dynamics of retail payments security, economics provides a useful framework. Economic principles that characterize retail payments security enable us to identify both drivers of and barriers to security investment and coordination in the industry. Applying game theory to payment security decisions reveals sources of conflicts among industry participants, and whether security strategies, technical solutions and policies employed by industry participants and policymakers can achieve security goals. If the results suggest those strategies, solutions, or policies

would be unlikely to achieve the goals, this approach also enables us to consider which part(s) of the game needs to be modified to achieve the desired level of security, providing insights into public policy and private entities' strategies.

The goal of this paper is to demonstrate how economic analyses can help to better explain coordination challenges facing payments security and strategies that produce socially desirable levels of payment security. Section II documents economic principles that underpin retail payments security. Section III describes how the game theory approach can be used to evaluate and construct security strategies. Section IV applies this approach to several case studies to evaluate actual technical solutions, both successfully and unsuccessfully implemented. Section V provides a summary and discussion on the role for policymakers to consider payments security from a broad and long-term perspective.

II. Economic principles related to retail payments security

Retail payments markets can be characterized by several economic principles. Basic principles that characterize retail payments markets in general include network externalities, two-sided markets and economies of scale and scope. Additional economic principles characterize retail payments security more specifically. These key principles include jointly produced goods, competition *for* the market, asymmetric information, moral hazard and trade-offs between information sharing and privacy. This section first describes basic economic principles that characterize retail payments markets. It then provides definition of each key principle related to payments security, describes how the principle and payments security are related, and discusses the implications on the incentives of various payments users and industry participants to align so as to produce socially desirable payments security.¹

II.i Basic economic principles that characterize retail payments markets

II.ia Network externalities

An externality exists when an individual agent's action affects other parties' benefits or costs that are not reflected in the prices of the goods or services involved. As a result, an individual agent's private benefits or costs do not coincide with the benefits or costs to society as a whole. Network externalities are one type of externality.² When this type of externality is

present, the value of a product or service for an individual consumer is dependent on the number of other consumers using it. For example, as more people adopt ATMs, more ATMs may be deployed and the number of ATMs available to an individual consumer may increase, and thus the value of ATM service for an individual consumer increases.

Payment innovations typically need to achieve “critical mass,” a sufficient number of adopters so that the rate of adoption becomes self-sustaining and creates further growth. If multiple providers in a network market compete for their customers with their new services, the degree to which providers’ services are interoperable could be an important determinant of whether the services can achieve critical mass. If those providers are effectively interoperable, then the services may achieve critical mass relatively easily because interoperability allows customers of alternative providers to exchange payments with each other.

To achieve critical mass as quickly as possible, competing providers may prioritize growth over any other goal, such as security (Levitin). For a new payment method, end-users’ concerns over its security are a barrier to adoption. However, once the method overcomes that concern, end-users tend to care about convenience of the method more than its security (Schuh and Stavins). This leads to payment providers’ focusing on enhancing convenience rather than improving security of the payment method.

II.1b Two-sided markets

In a two-sided market, end-users are divided into two distinct groups. In payment markets, one side of users are payees, such as merchants, and the other side are payers, such as consumers. Two types of externalities exist in two-sided markets because decisions of one side of users affect the value of the product or service to the other side of users.

The first type is adoption externalities, or cross-side network effects, which exist when a market is at its infant stage. In order for a new payment method to achieve critical mass, it needs to overcome a chicken-and-egg problem: enough payees must accept the new payment method for payers to use that method, and enough payers must use that method for payees to install the necessary hardware or software to accept that method.

The second type of externalities is usage externalities, which exist even in a mature market where critical mass has been reached or exceeded. For

example, a consumer's choice of payment method for a transaction at a merchant will affect the merchant's cost and benefit from that transaction. When the consumer decides which payment method to use, he typically does not take into account the merchant's cost or benefit from the transaction, unless there is a mechanism to incorporate the merchant's cost or benefit, such as surcharges and discounts offered by merchants to their customers based on payment method.

II.ic Economies of scale and scope

Production technology that requires significant capital investment often yields increasing returns to scale. As more quantities are produced in a plant, costs per quantity are reduced. In the payment industry a large share of costs is fixed and thus as one provider processes a larger volume of payments, its average cost per payment becomes lower than that of other providers.

Multiple types of payments can be effectively supported by an integrated infrastructure. Compared with entities that specialize in a limited service, entities that play multiple roles, such as network switches and processors for issuers and merchants, likely have lower average cost per payment by exploiting economies of scope. They may have separate physical platforms to play different roles, but other components necessary for payment processing, such as communication protocols, can be used to produce various services, thereby reducing the costs.

The presence of large economies of scale and scope in processing payments may inhibit entry and lead to payment markets in which a small number of large firms operate. This may be cost-effective, but may also give these firms significant market power, which may lead to monopoly or near-monopoly pricing and provide insufficient incentive for innovation.

II.ii Key economic principles related to retail payments security

II.iii Jointly produced goods

The strength of payment security is the result of efforts by all participants—not only by entities in the payment supply chain but also end-users—and thus is a jointly produced good. The contribution of each participant's efforts to secure payments is a function of the efforts of other participants. This interdependency implies the potential for coordination failure. Thus, without proper coordination of participants, the level of effort and the resulting strength of payments system security are more likely to be inadequate.

Protection of payment card data from breaches is a good example of jointly produced goods. Currently, sensitive payment card data are exchanged among entities in the payment card processing chain, including merchant, merchant processor, acquirer, card network, issuer processor and issuer. All of these entities' actions are important to protect payment card data from breaches.³ To coordinate their actions, the four U.S. credit card networks, along with the Japan Credit Bureau, established the Payment Card Industry Security Standards Council (PCI SSC).⁴ The PCI SSC develops and maintains the PCI Data Security Standards (PCI DSS) as a framework for prevention, detection and reaction to security incidents. The framework includes an audit function, enforced by each of the card networks, where any entity that stores or transmits sensitive card data must evaluate compliance with the standard.⁵

Many security technologies and protocols require joint adoption by industry participants. For example, both the payer's and payee's payment service providers need to adopt the same encryption standard so that they can read payment instruction and response. Encryption is used to secure sensitive payment data by transforming plain text information into non-readable information. A key (or algorithm) is required to decrypt the information and return it to its original plain text format. Coordination is essential for industry participants to decide which encryption standard to adopt and avoid a chicken-and-egg-problem: both the payers' and payees' service providers may wait to adopt the encryption standard until their counterparts adopt it.

Payment security is designed for defense-in-depth: if one defense is compromised, other defenses may mitigate losses. Although this design is beneficial, it may also cause free-rider problems whereby some industry participants may choose not to leverage useful defenses and instead rely on defenses provided by other industry participants. Thus, without coordination, investments in certain defenses or by certain industry participants may be inadequate.

II.iib Competition for the market

Profit-oriented firms may compete for the market by employing proprietary security standards rather than participating in open, consensus-based standards development. Although proprietary security standards may support incentives of firms to innovate, they may reduce interoperability. They also may be less secure in that security mechanisms designed in secret do

not benefit from an open vetting process to spot bugs prior to deployment. Open, consensus-based standards, on the other hand, are more likely to achieve interoperability by increasing industry participants' willingness to comply with the standards and thus exploit positive network effects (Greenstein and Stango). But they may take longer to develop and may not support innovation incentives. Neither type of standard-setting process can avoid coordination problems.

A good example of proprietary security standards is Europay, MasterCard and Visa (EMV) chip technology. EMV is a set of standards developed and maintained by EMVCo, which is owned by the global card brands. EMV uses the concept of dynamic data to strongly authenticate each and every transaction to mitigate counterfeit fraud in the card present environment.⁶ The proprietary nature of the technology standard, coupled with a unique requirement in the U.S. debit card industry—specifically, that a debit card carry at least two unaffiliated card networks to process transactions on the card—has provided global brands such as Visa and MasterCard a competitive advantage over U.S. PIN debit networks. Visa and MasterCard, by virtue of their ownership of EMVCo, could have met the requirement by making their chip available only to each other, or to a subset of PIN debit networks they select. After a long debate among card networks, Visa and MasterCard eventually made a series of bilateral agreements with each PIN debit network. While these agreements preserve the interoperability among PIN debit networks, reaching the solutions took a long time.

Another example is “tokenization” developed by EMVCo. A token, which replaces the payment card account number, is used for transactions made at a particular online merchant or mobile wallet provider (for example, Apply Pay). The token and card account number pair is stored on a highly secure server called a “vault.”⁷ Although this tokenization uses open standards, due to the proprietary environment in which the standards were developed, global card brands may have a competitive advantage at least initially in offering vault services compared with U.S. domestic card networks or processors.

II.iic Asymmetric information

Asymmetric information is a situation in which one party has more or superior information than the other. For example, a seller of security products may assert its product is more secure than the other products, but if potential buyers cannot verify it, sellers with better security products are

unable to differentiate their product from other, less-secure products. As a result, suppliers of security products have little incentive to produce a better product (Anderson).⁸

Asymmetric information may also exist between industry participants and regulators. Industry participants, such as card networks, have more and better information about security technologies, protocols and standards that are used in their day-to-day operation, while regulators may not have expertise to assess their effectiveness. Thus, regulators' security guidelines are often non- or less-prescriptive, allowing industry participants to select the security tools that they perceive as effective.

Information asymmetry can be seen in the reporting of costs of fraud or data security incidents. Many industry participants have an incentive to underreport those incidents. Banks and merchants may not want to reveal fraud losses for fear of frightening away customers using certain payment methods (such as cards) or channels (such as online). They may also not want to reveal data security incidents because of reputational risk. Operators of payment infrastructures may not want to reveal information on outages caused by malicious attack for fear it would draw attention to systemic vulnerability. On the other hand, other industry participants may have an incentive to overstate the aggregate losses in the industry. For example, security vendors may induce their customers to purchase their security services or products by overstating potential losses.

The lack of information about true costs of fraud or data security incidents prevents industry participants from accurately understanding threats and defenses. As a result, security investments may not be properly distributed across appropriate defenses.

II.iid Moral hazard

Moral hazard occurs when one person or party takes more risks because someone else bears the burden of those risks. Improper allocation of liability for fraud losses or data breaches discourages security investments made by parties that are best positioned to control the security. An example is a current lack of adoption of strong authentication methods for card-not-present (CNP) transactions, such as for online transactions, which impose a heavier fraud liability to merchants than to card issuers. Although card issuers could play more active roles in authenticating cardholders for online transactions, many U.S. card issuers currently do not do so, partly because the issuers do not bear most of the CNP fraud losses.

Data breach cost allocation may be another example of potential moral hazard or incentive misalignment. When a data breach occurs at a merchant, costs to compensate damages of the data breach to cardholders and card issuers are generally borne by the merchant and are not shared with its acquirer, who is responsible for ensuring their merchants are PCI compliant. But if some data breach costs are shared with acquirers, they may be more thorough in ensuring their merchants consistently comply with PCI DSS.

II.iiie Trade-offs between information sharing and privacy

Managing payments security is information intensive. As industry participants share more detailed information, the information becomes more actionable and helps mitigate payment security risks more effectively. But at the same time, the detailed information may raise privacy concerns.

An aggregate, accurate view of payment security incidents, losses, and causes over time would be valuable to better understand threats and defenses, enabling industry participants and policymakers to make informed decisions on security investment or policy. Other types of data sharing activities address data security, cyberattack, or fraud more directly. For example, Financial Services Information Sharing and Analysis Center (FS-ISAC) was formed to identify threats, coordinate protections against those threats and share information pertaining to both actual and potential physical and cybersecurity threats. Card networks and other payment service vendors use “big data” for neural network intelligence to detect suspicious transactions.

Some data sharing activities are successful, while others have struggled to overcome barriers to cooperation. Cyberthreat sharing may be viewed as one of the most successful examples of information sharing in the payment industry. Besides financial institutions, payment processors formed their own ISAC as a subgroup of FS-ISAC. Trade associations representing the merchant and financial service industries formed a cybersecurity partnership to share threat information, disseminate best practices for cyberrisk mitigation and promote innovation to enhance security. More detailed and particular information than that currently shared may make cyberthreat information more effective and actionable; however, sharing such information may require a safe harbor agreement. For example, a regulation or a rule on privacy protections can specify conditions under which specific data sharing activities will be deemed not to violate a given regulation or rule.

Data on payment fraud are collected and analyzed within large organizations, such as large financial institutions and global card

networks, but such data are not shared broadly. Although the Federal Reserve has started collecting some fraud data in its triennial payment study, they are very high level and may not be detailed enough or available in a timely manner to be actionable. Organizations may hesitate to share fraud data because doing so may expose the organizations to reputational risk and have privacy implications.

To detect suspicious transactions, neural network intelligence is used along with, or as a substitute for, stronger payer authentication. The neural network intelligence leverages “big data,” such as payers’ spending patterns and geographical areas, to flag payments outside of a specific payer’s “norm.” The data may be effective to mitigate payment fraud, but they raise privacy concerns because the data include detailed behavioral information about individual consumers.

III. Strategies to achieve desired payments security—game theory approach

In considering payments security strategies, a game theory approach would be useful. To examine whether the current market structure will be able to develop, implement, and adopt a specific security technology, method, or protocol, the game theory approach defines actual players, their preferences, rules of the game including actions available to each player and outcomes of the game. If the results suggest the current market would be unlikely to achieve the goal, this approach also enables us to consider which part(s) of the game needs to be modified to achieve the desired level of security, providing insights into public policy and private entities’ strategies.

III.i Game theory

Game theory is the formal study of conflict and cooperation. Game theory can be applied whenever the actions of two or more entities—individuals, organizations, governments—are interdependent. These entities make choices among actions in situations where the outcomes depend on the choices made by both or all of them and each has his, her, or its own preferences among the possible outcomes. The concepts of game theory are useful to understand, analyze, structure, and formulate strategic scenarios. Readers familiar with game theory can skip this subsection and resume in subsection III.ii where applications to payments security are presented.

A game is a formal model of an interactive strategic situation. It typically involves two (or more) players, their preferences, their information, their

Figure 1
2-player, 2-action Game

		<u>Player 2</u>	
		Left	Right
<u>Player 1</u>	Up	A, a	C, c
	Down	B, b	D, d

Figure 2
Numerical Example of 2-player, 2-action Game

		<u>Player 2</u>	
		Left	Right
<u>Player 1</u>	Up	10,5	0,0
	Down	0,0	5,10

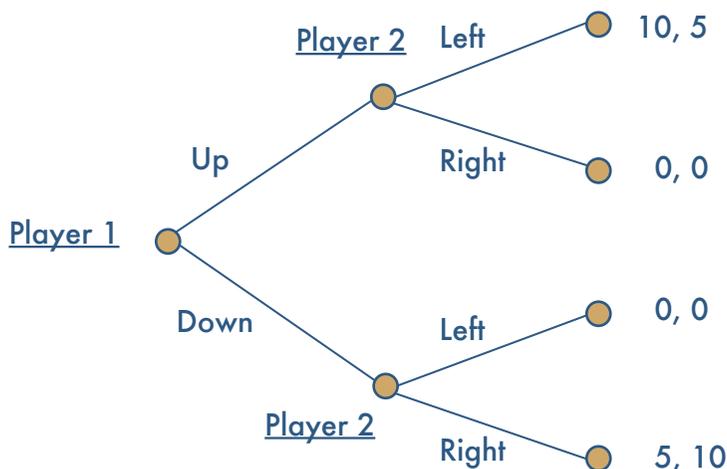
available actions and outcomes represented by a separate payoff for each player. In a game, the outcomes and the actions available to the players are assumed to be common knowledge. In other words, each player knows not only his own payoffs and actions but also the other players' payoffs and actions. Typically, each player is assumed to be rational and always chooses an action which gives the outcome he most prefers (or the highest payoffs), given what he expects his counterparts to do.⁹

To describe a 2-player, 2-action game, the *strategic form* (also called *normal form*) is typically used (Figure 1). In this game, Player 1 has two actions to choose from—Up or Down—and Player 2 also has two actions—Left or Right. When Player 1 chooses Up and Player 2 chooses Left, the strategy profile is denoted as (Up, Left), and the payoff of that strategy for Player 1 is A and that for Player 2 is a.

In a game theory, an equilibrium (often called Nash equilibrium) is the set of choices of each player that provides the maximum payoff to the players given what they believe about the other players' beliefs, and all players' beliefs are rational.¹⁰ The equilibrium depends on both *actions* and *beliefs*, and is stable because all players have the same information and the actual choices coincide with the beliefs of the players.

Consider a numerical example in Figure 2. Player 1 chooses his action based on his beliefs about Player 2's behavior. Suppose Player 1 believes

Figure 3
Sequential Game (extensive form)



Player 2 chooses Left, then he chooses Up, because his payoff is higher by choosing Up than by choosing Down (10 vs. 0). And his belief about Player 2 is reasonable: if Player 2 believes Player 1 chooses Up, then she chooses Left because her payoff is higher by choosing Left than by choosing Right (5 vs. 0). Since each player's belief about the other player's choices coincides with the actual choices the other player intends to make, (Up, Left) is an equilibrium of this game. Another equilibrium exists in this game. Suppose, Player 1 believes Player 2 chooses Right, instead. In this case, Player 1 chooses Down, because his payoff is higher by doing so than otherwise (5 vs. 0). His belief about Player 2's action is also reasonable because if Player 2 believes Player 1 chooses Down, then her choice is Right, rather than Left. Again, each player's belief about the other player's choices coincides with the actual choices the other player intends to make, and therefore, (Down, Right) is an equilibrium as well.

The example in Figure 2 describes a case where both players make their choices simultaneously. But what if Player 1 chooses his action before Player 2 and Player 2 chooses action after knowing Player 1's action? To describe a sequential game, a *game tree* (also called *extensive form*) is used (Figure 3). A choice in the game corresponds to the choice of a branch of the tree and once a choice has been made, the players are in a *subgame* consisting of the strategies and payoffs available to them from then on. If Player 1 chooses Up, it will be optimal for Player 2 to choose Left, which gives a payoff of 10 to Player 1. If Player 1 chooses Down, it will be optimal for

Player 2 to choose Right, which gives a payoff of 5 to Player 1. Player 1 is better off by choosing Up than Down, and thus, (Up, Left) is the equilibrium for this sequential game. Unlike the simultaneous-move game above, Player 1 does not have to consider the possibility that Player 2 chooses Right because once Player 1 chooses Up, the optimal choice in the resulting subgame is for Player 2 to choose Left.

III.ii Applications to payment security

Both the strategic form and a game tree can be used to conceptualize coordination problems the payment industry faces to achieve high level of security. Some coordination problems are relatively easy to solve, while others are more complicated.

As an easy coordination problem, consider a game shown in Figure 4. In this game, two players choose to adopt either one of two security technologies: Technology 1 or Technology 2. Both technologies require joint adoption by both players to be effective. Technology 1 is superior to Technology 2, in terms of its effectiveness of making payments secure or its costs of initial investments and ongoing operation incurred by each of the players. In this game, (Technology 1, Technology 1) and (Technology 2, Technology 2) are equilibria, although the former provides higher payoffs to both players than the latter. It may be easier to reach the equilibrium which provides higher payoffs to both players than the other equilibrium. Since both players have no incentive to deviate from cooperation, either or both of the players can provide their true preference for technology before the game. Or a regulator's non-prescriptive guidance in encouraging industry participants to adopt "stronger" security may be sufficient to reach the equilibrium of (Technology 1, Technology 1).

The second example is the same as above except that both technologies are equally effective (Figure 5). Two equilibria exist for this game, and both equilibria are equally preferred by both of the players. In this case, a regulator's non-prescriptive guidance may not help select one of the two equally effective technologies to adopt in the industry. But the industry can easily select either one of the technologies by negotiating which technology to pick.

A third example shows the case where reaching one solution is more complicated than the previous two examples (Figure 6).¹¹ The payoffs of this game are exactly the same as the numerical example shown in Figure 2. Like the previous two examples, the two technologies require joint adoption. But in this game, payoffs are asymmetric. Among the two equilibria, Player 1 prefers both players adopt Technology 1, while Player 2 prefers both players adopt

Figure 4
Security Technologies that Require Joint Adoption

		Player 2	
		Technology 1	Technology 2
Player 1	Technology 1	10, 10	0, 0
	Technology 2	0, 0	5, 5

Figure 5
Equally Effective Security Technologies that Require Joint Adoption

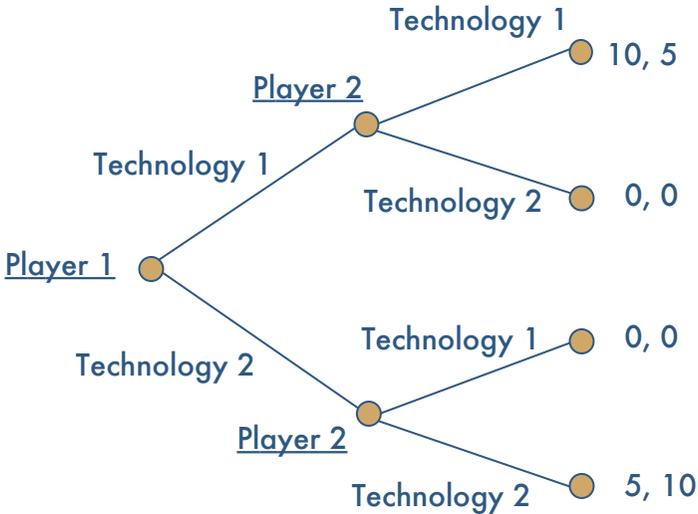
		Player 2	
		Technology 1	Technology 2
Player 1	Technology 1	10, 10	0, 0
	Technology 2	0, 0	10, 10

Figure 6
Asymmetric Payoffs with Security Technologies that Require Joint Adoption: Simultaneous Move Game

		Player 2	
		Technology 1	Technology 2
Player 1	Technology 1	10, 5	0, 0
	Technology 2	0, 0	5, 10

Technology 2. Unlike the example shown in Figure 5, industry negotiation may not be easy unless one player has stronger bargaining power than the other. Or alternatively, if one player can move before the other player, they can reach one equilibrium (Figure 7). In this case, the first mover (say, Player 1) has the advantage and chooses the technology the first mover prefers. Since the second mover is better off by choosing the same technology the first mover chose rather than by choosing the other technology, this sequential game has one equilibrium, in which both players' adopting the technology the first mover prefers.

The next example is the case where one technology requires joint adoption, but another technology does not require joint adoption (Figure 8).¹² The technology requiring joint adoption (Technology 1) is more effective in securing the payments system than the technology that does not require

*Figure 7***Asymmetric Payoffs with Security Technologies that Require Joint Adoption: Sequential Game**

joint adoption (Technology 2). Two equilibria exist in this game: both players' adopting Technology 1 or both adopting Technology 2. Similar to the first example, both players prefer both adopting Technology 1 over both adopting Technology 2. Nevertheless, the coordination may be more difficult in this example than the first example. The problem here is the riskiness of adopting Technology 1. While adopting Technology 2 guarantees a payoff of 7 for both parties, adopting Technology 1 provides either 10 or 0. For this reason, both players might choose the less risky Technology 2.

III.iii Tools to influence the game

The previous two subsections consider the structures of games, such as players, their available actions, sequence, and payoffs, are given. In reality, however, the structures can be changed. Myerson (2009) suggested necessary steps to change the structure of a game so that the players of the game can achieve collective action. The structures of games are influenced by various factors, including pricing, liability distribution, industry requirements, regulatory mandates, subsidies and property rights. By using these factors as tools, regulators and payments system operators can change the structures of games to overcome coordination problems.

Figure 8
Security Technology that Requires Joint Adoption vs. One That Does Not

		Player 2	
		Technology 1	Technology 2
Player 1	Technology 1	10, 10	0, 7
	Technology 2	7, 0	7, 7

Regulatory mandates and industry requirements, for example, may limit actions available to players. They may also change the sequence of a game, so that the game provides a level playing field for every player. Subsidies, liability distribution and pricing can be used to change payoffs. Subsidies from government or card networks may be provided if players select socially desirable actions, enticing each player to select those actions. Heavier fraud or data breach liability may be imposed on players if they select actions that are not socially desirable. Pricing, such as interchange fees, can be structured so that players who adopt stronger security technology or protocols are more rewarded than those who do not. Property rights or standard setting may affect payoffs as well as sequence of games. Having consensus-based standards, rather than proprietary standards, may distribute payoffs more evenly across different players and eliminate the first mover advantage to players who have property rights versus players who do not.

To illustrate the value of modeling payments security scenarios using game theory, consider the EMV migration currently under way in the United States. At the time of writing, issuers are generally liable for card-present (CP) fraud.¹³ In October 2015, the fraud liability for a CP transaction will shift to the merchant if the merchant does not adopt EMV but the issuer does.¹⁴ If neither or both parties adopt EMV, then the fraud liability will remain as it is today.¹⁵ How the liability shift incentivizes merchants to adopt EMV and changes equilibrium can be demonstrated in a game theory framework.

Both before and after the liability shift, issuers and merchants have a choice of whether they adopt EMV or not. Figures 9 and 10 represent hypothetical payoff matrices for EMV adoption before and after the liability shift.¹⁶ In both figures, the payoffs are set relative to the status quo of issuers distributing magnetic stripe cards and merchants not deploying EMV terminals. Suppose EMV adoption by both issuers and merchants will reduce CP fraud by 4 in value. Suppose also EMV adoption will require issuers and merchants respectively to spend additional cost of 2. For

Figure 9
Hypothetical Payoff Matrix for EMV Adoption Before Liability Shift

		Adopt EMV?	
		Issuer	
		No	Yes
Adopt EMV? Merchant	No	0, 0	0, -2
	Yes	-2, 0	-2, 2

example, the additional cost for issuers includes the cost of issuing EMV cards relative to that of issuing magnetic stripe cards. Similarly, the additional cost for merchants includes the cost of deploying EMV terminals relative to the cost of deploying terminals that can read magnetic stripe cards only.

Before the liability shift, merchants always choose not to adopt EMV regardless of issuers' choice (Figure 9). If merchants adopt EMV, they incur the additional cost of 2. Even if issuers also adopt EMV, merchants do not receive any benefit from the reduced CP fraud because issuers are liable for CP fraud. Thus, merchants' net payoff is -2 when they adopt EMV regardless of issuers' choice. If merchants do not adopt EMV, then they do not incur additional cost at all and thus their net payoff is zero. Given merchants always choose not to adopt EMV, issuers also choose not to adopt EMV. By adopting EMV, issuers incur the additional cost but they cannot reduce CP fraud because merchants do not adopt EMV. Hence, their net payoff is negative. On the other hand, if issuers do not adopt EMV, they incur no additional cost and thus their net payoff is zero. In this game, the only equilibrium is both issuers' and merchants' not adopting EMV.

After the liability shift, merchants are liable for CP fraud if they do not adopt EMV but issuers do. The only outcome where payoffs change from Figure 9 to Figure 10 is (No, Yes) strategy profile, that is where merchants choose not to adopt EMV and issuers choose to adopt EMV. In this case, merchants' net payoff is -4: although merchants incur no additional cost for terminal deployment, they incur CP fraud losses of 4, the liability shifted from the issuers. Under the modified payoff matrix, the only equilibrium is now (Yes, Yes). Hence, in a situation where payment card networks can alter liability distribution, they can influence payoffs in a way that encourages the adoption of secure technologies.

It is worth noting that while the payment card networks' liability shift

Figure 10
Hypothetical Payoff Matrix for EMV Adoption After Liability Shift

		Adopt EMV? Issuer	
		No	Yes
Adopt EMV? Merchant	No	0, 0	-4, -2
	Yes	-2, 0	-2, 2

will likely generate the more secure outcome, it may not distribute the net benefit equally to the involved parties. Indeed, the equilibrium payoff for merchants in the game after the liability shift is less than that in the game before the shift. However, it is difficult to infer the fairness of this liability shift from these payoffs for a few reasons. First, since the payoffs in these games are set relative to the status quo, the actual payoffs in absolute term are unknown. Thus, this unequal net benefit distribution could worsen, or improve, the distribution of initial payoffs in absolute term between merchants and issuers. Second, potential indirect benefits of EMV migration are disregarded in these games. For example, if EMV migration will increase the share of transactions made with PIN, merchants will reduce interchange fee payments to issuers. The EMV migration may also facilitate mobile payment adoption, which may benefit merchants and issuers. Third, as these games indicate, even if merchants incur the heavier burden than issuers for EMV migration, merchants may incur the lighter burden than issuers for other complementary security improvements, such as stronger authentication for CNP transactions. It is important for entities that can influence the structure of coordination games, such as regulators and payments system operators, to have security strategies with a broad scope so that the costs and benefits of security improvements as a whole—rather than those of a single security improvement—can be distributed fairly among the involved parties.

IV. Case studies

Fraud, data breaches and other security incidents should be minimized in a cost-effective manner in order to maximize the social benefit of payments. In principle, this could be achieved if the payment participant in the best position to prevent these incidents took steps to detect and deter them. In the ideal world, the best positioned payment participant has enough incentive to balance the incremental costs of security against the incremental reduction

in fraud, data breaches and other security incidents. Public and private entities ensure payment security by increasing incentives among industry participants to secure data and deter fraud. They enforce laws and contractual rules (sometimes embedded in operational procedures) through mechanisms such as regulations, supervision and audits (Sullivan). In reality, however, it is not easy to coordinate industry participants and align their private incentives so that private benefits and costs correspond to social benefits and costs. When private benefits or costs are not aligned with social benefits or costs, the level of security is typically not at the socially desirable level.

Four case studies illustrate situations where incentives appear insufficient to adequately secure payments. In some markets, however, incentive misalignment has been reduced due to coordinated efforts led by public authorities or among industry participants voluntarily, while in other markets incentive misalignment remains unaddressed. Each case study identifies economic principles that explain incentive misalignment or sources of conflict to make coordinated efforts among industry participants for payment security difficult. It also describes whether and how the coordinated efforts have reduced conflict or incentive misalignment.

The first concerns fraud in CNP payments, such as online payments where the card is not physically presented to a merchant. Because access to the card is eliminated, the merchant cannot authenticate the card or the buyer's signature, leading to high rates of fraud losses. Systems to improve CNP payment authentication have been available for many years but have not been widely adopted in the United States.

The second case study illustrates inadequate protection of sensitive payment data that is useful for committing payment fraud. Despite card brands creating institutions to encourage strong security over sensitive data, card accepting merchants and card payment processors have been victims of successful attacks that penetrate computer system defenses and allow unauthorized access to sensitive data. The expectations for card payment security has been ratcheted up over time yet data breaches appear to be more frequent and expose more data. There is some evidence showing higher rates of compliance with security standards recently yet data breaches continue to grow.

Mobile payments are the third case study. This emerging payment method, or form factor, offers the promise of improved security through

the use of tokenization. However, adoption remains low. One explanation for the slow uptake is that the new stakeholders are involved (device manufacturers and carriers), and they are fiercely competing for the market even when it comes at the expense of network effects needed to achieve widespread adoption. Unresolved tussles over who gets to control payment metadata also threaten adoption. Moreover, early evidence suggests fraud rates exceed existing methods.

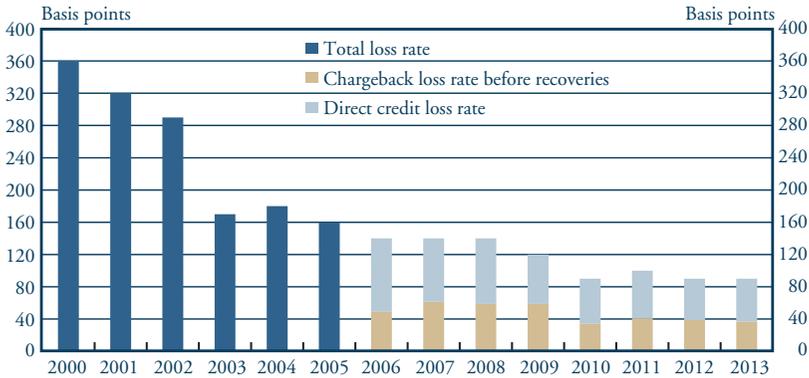
The fourth case study, cryptocurrencies, demonstrates security that is, in some respect, more secure than existing payment methods in that no sensitive account information is transmitted with payments. They may also be the most “disruptive” challenger to existing payment networks. Payment processing services make it easy for merchants to accept payments in bitcoin, and do so at very attractive terms to merchants: zero transaction fees and non-revocability. Nonetheless, significant barriers remain. Consumer incentives to adopt cryptocurrencies for payments are weak, with the exception of international payments in the remittance market. Operational risks due to widespread fraud (both payment fraud and broader financial fraud) could inhibit adoption, particularly when compared to the consumer protections available in traditional payments.

IV.i Reducing fraud in CNP payments

CNP payments, where the merchant sees neither the payment card nor the cardholder, have high fraud loss rates. A recent survey of U.S. and Canadian Internet merchants suggests a loss rate of 38.7 basis points (0.387 percent) on the value of sales in 2013 for chargebacks, which are transactions reversed by the card issuer, as fraudulent (CyberSource 2015).¹⁷ The survey also reports an average 51.3 basis point (0.513 percent) loss of the value of sales for refunds provided to customers who contact the merchant, instead of their issuers, to report unauthorized transactions (Chart 1).¹⁸ In this case, merchants credit directly to the customer’s payment card account.

To combat fraud, Internet merchants review a range of information to evaluate whether a transaction is trustworthy. Merchants commonly verify payment card numbers, customer addresses and phone numbers, as well as consult their own records for a history of serving customers. These measures have helped to bring the fraud loss rate down since 2000 but it still remains high (Chart 1).

The fight against fraud in CNP payments is an urgent matter in the

Chart 1**Fraud Loss Rate on Value of Internet Transactions, United States**

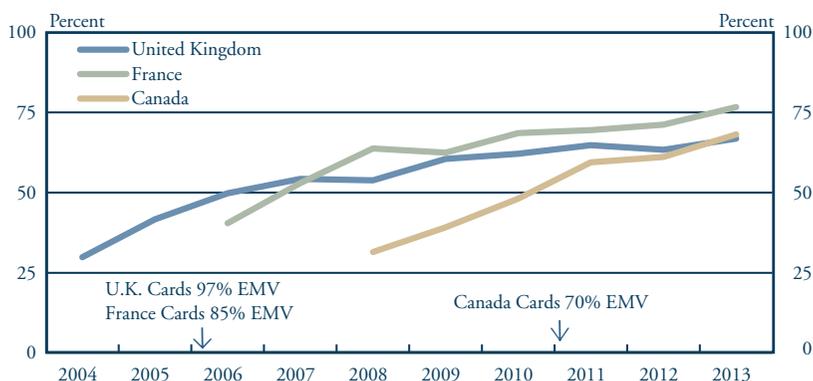
Source: CyberSource (various years).

United States for two reasons. First, CNP payments, especially in Internet commerce, will continue to expand and thus transfer transactions from relatively safe brick-and-mortar locations to the more fraud-prone online marketplace. Second, and more important, in 2015 the United States will begin to deploy new payment cards that contain an EMV chip. These chip cards will cut off counterfeit payment cards in the United States, a leading cause of fraud transactions on card payments.¹⁹ When the cardholder also enters a PIN to initiate a payment at brick-and-mortar locations, the chip card also prevents fraud on lost or stolen cards.²⁰

The rest of the world has moved to chip cards, and in many countries fraud shifted to channels with relatively weak security. Fraud increased dramatically in CNP transactions such as Internet, mail order and telephone order purchases, where cardholder authentication is weak because the payment card is not physically presented to the merchant. The United Kingdom, France and Canada each experienced substantial increases in fraud on CNP transactions, which became the leading source of fraud on card payments soon after introduction of chip cards (Chart 2). It is likely the United States will have a similar experience.²¹

The difficulties of authenticating payment cards and cardholders in CNP payments contribute significantly to these losses. Because an Internet merchant has little reliable evidence of who initiated the purchase, it cannot easily dispute a fraud chargeback or counter the claim of a customer who denies making an online purchase.²²

Chart 2
CNP Fraud Share in Card Payment Fraud Losses
United Kingdom, France and Canada



Sources: Financial Fraud Action; Canadian Bankers Association, Credit Card Fraud Statistics; OPCS; Lucas (2011).

Authenticating a cardholder in CNP transactions can be improved by adding a step to payment initiation. To initiate a transaction, the cardholder enters a password, which is previously shared with his card issuer, or a special code received from his card issuer. Because only the cardholder would know the password or code, it adds assurance that the cardholder truly initiated the transaction.

Two common methods of enhanced authentication are 3D Secure (3DS) passwords, offered by the major payment card brands, and single-use codes sent to the cardholder via text messages, available from a variety of processors. The 3DS system requires a cardholder to register with the program and create a password that is used solely for CNP transactions. A cardholder must also register for single-use code authentication systems and have a mobile device to receive the code.²³

Available in the United States since 2003, 3DS has gained little traction. In 2013, only 21 percent of merchants responding to a survey reported using 3DS for Internet transactions. Survey estimates of adoption rates among merchants in 2013 range from 3 percent to 21 percent (TSYS; CyberSource 2015).²⁴ Adoption has lagged despite evidence that enhanced authentication has proven effective at reducing payment fraud in Internet transactions in France (OPCS 2013a). The puzzle is why it is not more widely adopted in the United States.

An important reason is that incentives to adopt are misaligned.²⁵ Card issuers absorb fraud losses in CP transactions and thus take advantage of physical authentication (signature or PIN) to deter fraud. But card issuers do not absorb the loss on fraudulent CNP transactions and thus do not have much incentive to enhance authentication. Merchants, on the other hand, in the absence of wide-scale adoption, fear that the extra steps in the checkout process required by enhanced authentication will cause customers to abandon an online shopping cart and make their purchases elsewhere. Indeed, a recent study reports cart abandonment in 3DS transactions is over 40 percent in the United States (Adyen), a substantial disincentive for merchants to adopt the system.²⁶ Because everyone would be better off if everyone is collectively switching to a stronger authentication process, the current misalignment of incentives—no parties have a strong incentive to be the first party to make changes—is an example of a chicken-and-egg barrier.

This chicken-and-egg barrier can be illustrated in a game theory framework. Consider a game in which two merchants compete in the circumstance where issuers' 3DS adoption rate is quite low and a merchant's adoption of 3DS does not shift fraud liability to issuers (Figure 11). Suppose that a merchant can reduce CNP fraud by 2 by adopting 3DS but it may lose sales by 3 to its rival merchant if the rival merchant does not adopt 3DS.²⁷ The payoffs for both merchants are higher when both adopt 3DS than when neither adopts it; nevertheless, they cannot reach that outcome because a merchant is better off by not adopting 3DS when its rival accepts it.

Consider another two-merchant game when the benefit of 3DS exceeds the cost of forgone business. This could be achieved by either a higher 3DS adoption by issuers or by shifting liability to issuers for potential 3DS transactions, or both (Figure 12). Merchants can now reduce CNP fraud by 4 by adopting 3DS, but it may still lose sales by 3 to its rival merchant if the rival merchant does not adopt 3DS. In this game, the most secure outcome—both merchants' adopting 3DS—is the single equilibrium.

These two games suggest that if the benefit from reduced fraud by adopting 3DS exceeds the opportunity cost of lost sales, then the most secure outcome is the likely equilibrium.

Increasing issuers' adoption of 3DS is an important first step. The higher the issuers' adoption rate of 3DS, the greater the reduction in fraud losses incurred by merchants will be. This, in turn, could increase merchants' adoption of 3DS, and thereby diminish the opportunity cost of offering

Figure 11
Hypothetical Payoff Matrix for 3DS Adoption: Low Issuer Adoption Rate and No Liability Shift

		Adopt 3DS? Merchant 2	
		No	Yes
Adopt 3DS? Merchant 1	No	0, 0	3, -1
	Yes	-1, 3	2, 2

Figure 12
Hypothetical Payoff Matrix for 3DS Adoption: High Issuer Adoption Rate or Liability Shift to Issuers

		Adopt 3DS? Merchant 2	
		No	Yes
Adopt 3DS? Merchant 1	No	0, 0	3, 1
	Yes	1, 3	4, 4

3DS in terms of business lost to rivals. Hence the interaction between merchants and issuers exhibit substantial cross-side network effects in the two-sided market. Were issuers to assume liability for CNP transactions at merchants who adopt 3DS, this could make adoption more attractive to merchants. As more merchants adopt 3DS, more issuers are also willing to adopt 3DS.

The experiences of some countries can shed light on how greater adoption of enhanced online authentication might be encouraged. France and the United Kingdom have successfully increased adoption of 3DS and reduced their CNP fraud rates; however, approaches taken by these two countries were different. In France, the Bank of France and the Observatory For Payment Card Security (OPCS) played a leadership role, while in the U.K., participants in the payment card industry adjusted their behavior to new incentives created by rapidly rising CNP fraud losses with little involvement by public authorities.

In various ways, leadership of the Bank of France helped to promote collective action on CNP fraud. It tracked CNP fraud and revealed a growing

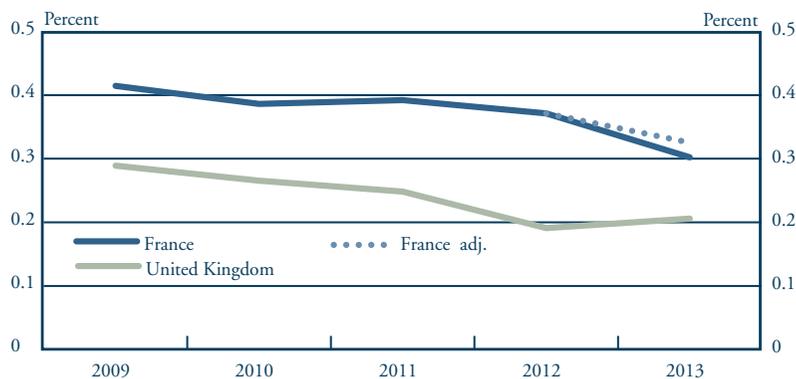
problem (OPCS 2008a). It researched options for securing CNP transactions and cited value of 3DS system in enhanced authentication (OPCS 2008b). It examined consumer attitudes toward security in CNP transactions (OPCS 2009). It engaged card issuers and merchants in a working group and partnered with payment participants to find ways to lower cart abandonment among consumers asked to use enhanced authentication in online transactions (OPCS 2010). Instead of being overly prescriptive in specifying the technology, the Bank of France let card schemes and issuers freely evaluate and implement forms of strong online authentication that best fit their needs (OPCS 2013b).

France has shown considerable progress with CNP fraud by adopting 3DS. In 2008, a significant number of card issuers began to accept fraud losses if the merchant used 3DS authentication for Internet transactions. Merchants and cardholders also took actions: in 2013, 95 percent of cardholders had access to enhanced authentication, and 43 percent of Internet merchants used it for transactions that account for nearly 30 percent of the value of Internet sales (OPCS 2013a). The fraud loss rate in Internet transactions fell steadily since 2009, to 0.29 percent of the value of transactions in 2013 (Chart 3).

In the United Kingdom, in contrast, concerted efforts of card issuers, card networks, merchant acquirers and merchants were drivers of 3DS adoption. Merchant acquirers provided incentives to merchants for adopting 3DS and for promoting cardholder enrollment in the system. Card networks and issuers developed an enhancement to 3DS so that merchants can flexibly decide when to use 3DS.²⁸ Computer analysis of payment at initiation is used to predict the likelihood of fraud. The merchant can choose the threshold for requiring 3DS, and if the risk of fraud on an enrolled card is low, the transaction would not require a password for approval but the merchant is still not liable for fraud (CyberSource U.K. 2012). Moreover, the simplified transaction process reduces the rate of cart abandonment. Interestingly, more recent estimates show that Internet shoppers in Great Britain are more likely to complete a purchase if the merchant uses 3DS (Adyen). The merchants' adoption of 3DS may have altered consumers' perceptions toward 3DS from negative to positive.

These initiatives reduced CNP fraud. About half of U.K. payment cards were enrolled in 3DS by 2011 (British Retail Consortium, private communication 2011). Nearly 70 percent of U.K. merchants used 3DS as one

Chart 3
Fraud Loss Rate on Value of Internet Transactions, France and the United Kingdom



Sources: Financial Fraud Action; U.K. Office of National Statistics; OPCS.

Notes: For 2013, the OPCS changed its method for calculating fraud on CNP transactions, which lowered the fraud rate on e-commerce transactions. The France adj. series shown makes a rough adjustment to obtain a fraud rate more comparable to previous years, and demonstrates that the continued downward trend in the loss rate is unlikely to be a result of the change in OPCS methods.

tool to combat card payment fraud in 2013 (British Retail Consortium 2014). Statistics on the U.K. fraud rate for Internet card transactions are less precise than those for France, but available data suggest a decline in the rate since 2009 (Chart 3).

In the United States, similar barriers to enhanced authentication are present and high rates of fraud in CNP transactions will likely persist without increased effort to make changes that properly align incentives. Like in the United Kingdom, Visa and MasterCard have recently taken important steps to reduce the burden of 3DS on merchants (Montague). First, in 2011, MasterCard joined Visa in shifting the liability of fraud for U.S. merchants to the card issuer for CNP transactions that go through the 3DS system. Second, rather than sending a customer to a card issuer's website to enter a 3DS password, merchants can now choose to present the password entry window on their own websites.²⁹ Third, merchants also have some control over what transactions go through 3DS. For example, a merchant can accept the payment of a customer it has served for a period of time without requiring 3DS. The merchant does not get a payment guarantee, but from its perspective the transaction has low risk and its longtime customer can enjoy a simplified checkout process.

Whether these changes are sufficient to drive U.S. adoption of enhanced online authentication of card payments is yet to be seen. Network effects in a two-sided market can be difficult to overcome when the current equilibrium is low adoption by both sides. Nonetheless, since large numbers of EMV cards will be distributed in 2015, the time is very short to get meaningful numbers of merchants, issuers and consumers to use enhanced authentication.

IV.ii Protecting sensitive data

Data breaches are a common but particularly damaging method of stealing card data.³⁰ Hackers access large numbers of payment card records from computer systems where the data is stored. The stolen card data can be used to create counterfeit payment cards useful in over-the-counter purchases. They can also be used to make CNP purchases.

To better protect payment card data, the major card brands joined in 2006 to establish the Payment Card Industry Security Standards Council (PCI SSC) as part of their risk control structure. The PCI SSC develops and maintains the PCI Data Security Standards (PCI DSS), and each card brand enforces compliance with the PCI DSS for entities that process its payments and for merchants that accept its cards. A tiered compliance system imposes stricter validation requirements on large, higher-risk merchants, which must engage independent validation assessors on at least an annual basis, but allows smaller merchants to perform self-evaluations. Large merchants are more likely to be validated as compliant with the PCI DSS than are smaller merchants. For example, in 2014, 97 percent of Visa's 450 largest merchants (Level 1), whose aggregated transactions accounted for 50 percent of Visa's U.S. transactions, validated as compliant with the PCI DSS (Table 1). The proportions of compliant merchants decline for smaller merchants (Levels 2-4).

High compliance validation rates among Level 1 and 2 merchants were achieved in the first few years after the card brands started enforcing PCI DSS in 2006 (Table 2). The compliance validation rates were 12 percent for Level 1 merchants and 15 percent for Level 2 merchants at the end of the first quarter of 2006, which increased to 91 percent and 87 percent, respectively, by the end of 2008. The compliance validation rate for Level 1 merchants has been higher than 95 percent for the past several years, while Level 2 merchants peaked at 99 percent in 2010 and then declined. The rate for Level 3 merchants has been lower: it has been around 60 percent

Table 1
PCI DSS Compliance Status for Merchants Accepting Visa Cards in 2014

Merchant Level (Annual Transactions)	Estimated Population Size	Estimated Share of Visa Transactions	PCI DSS Compliance Validation	Validated Not Storing Prohibited Data
Level 1 Merchant (>6M)	450	50%	97%	100%
Level 2 Merchant (1-6M)	972	13%	88%	100%
Level 3 Merchant (e-commerce only 20,000 – 1M)	4,095	< 5%	61%	N/A
Level 4 Merchant (<1M)	~ 5,000,000	32%	Moderate**	TBD

**As of June 30, 2014. Level 4 compliance is moderate among stand-alone terminal merchants, but lower among merchants using integrated payment applications.

Source: <http://usa.visa.com/download/merchants/cisp-pcidss-compliancestats.pdf>

for the last few years.

Despite the relatively higher compliance validation rates among larger merchants, data breaches that exposed millions of payment card accounts have occurred at several larger merchants in recent years. Among the largest U.S. breaches that exposed payment card data are the 2009 breach at Heartland Payment Systems (130 million records), the 2013 breach at Target Brands Inc. (40 million records) and the 2014 breach at Home Depot (56 million records). The total number of U.S. data breach incidents, which includes breaches that exposed non-payment card data, was 1,343 in 2014, up from just over 600 in 2009 (Sullivan; Risk Based Security). During the same period, the number of records exposed per year also increased from about 200 million to 512 million.

It is hard to reconcile a long-established audit regime for data security and high levels of compliance with an increasing stream of data breach reports. Part of the answer lies in the many economic challenges that the card brands face in developing a secure network, as outlined in Section II. These challenges suggest that misaligned incentives are playing a significant role in undermining the card brands' security control structures.

Four groups of entities are responsible for the design, implementation and enforcement of card payment security standards. The card brands, through the PCI Council, specify security standards and certify valida-

Table 2**PCI DSS Compliance Validation Rates for Merchants Accepting Visa Cards**

	2006	2008	2010	2012	2014
	Q1	Q4	Q2	Q2	Q2
Level 1 Merchant (>6 million annual transactions)	12%	91%	99%	97%	97%
Level 2 Merchant (1-6 million annual transactions)	15%	87%	99%	93%	88%
Level 3 Merchant (e-commerce only, 20,000 – 1 million annual transactions)	n.a.	n.a.	n.a.	60%	61%

tion assessors. Banks that offer merchant acquiring services (that is, card payment processing) monitor their merchant client operations, including tracking records of validation, and enforce fines or other sanctions for compliance violations. Third-party validation services assess large merchants for PCI DSS compliance, while smaller merchants assess themselves. Finally, merchants are responsible for implementing PCI DSS to secure the data used to process card payments.

Conflicts of interest may compromise incentives to protect card payment data among any of the four entities. The card brands and issuers place a high value on security but at the same time may choose convenience of the card payment process ahead of security (Huen). Merchant acquirers often include provisions in their contract that make merchants responsible for any fines that result from a failure to comply with PCI standards, which diminishes their incentive to closely monitor their clients. PCI validation services are relatively new, and assessors may be placing a high value on building their client list at the expense of thorough assessments, while self-assessments have an obvious conflict of interest.³¹ Merchants bear significant costs implementing PCI DSS but have seen penalties enforced on validated merchants after security failures, and may not see enough value in compliance to put much effort into protecting data.³² Finally, any of these four parties that suffer a breach may not have sufficient incentive to secure data if they are not held responsible for the costs of the damage that results from the breach.³³

By their nature, modern payment systems are large and complex, which makes the effort to ensure integrity very difficult. The PCI Council is clearly a step in the right direction. But the continued reports of unauthorized access

to sensitive data suggest that incentives to improve data security may not be strong enough to keep up with threats of data breaches. The card industry may be in a situation represented by a game shown in Figure 8 in Section III, which depicts an equilibrium with inadequate levels of security and little incentive for the parties to jointly adopt options with stronger security.

IV.iii Mobile payments

The mobile device form factor offers a promising opportunity to improve the security of electronic payments. Mobile wallet applications typically use methods and technologies that stronger authenticate the payer and payer's payment device and better protect sensitive data than those used by existing payment methods such as payment cards. This opportunity, however, comes at the cost of added institutional complexity to business models of mobile payment platforms. New players, such as mobile carriers and device makers, have joined the market with their own incentives. Carriers may want to be a tollbooth, charging a fee for transactions that take place on their networks. Device makers may want to construct a services platform in which they are in the middle. These competing interests turn out to have broad implications for the security technologies they propose, and especially their prospects for widespread adoption.

As compared to existing payment methods such as credit and debit cards and automated clearinghouse (ACH), mobile wallet applications will improve payment security by enhancing both payer authentication and data protection. Mobile payments could reduce the likelihood of unauthorized transactions through password or biometric protection of the mobile device and of the mobile payment application on the device. Such protection provides an extra layer of security that does not exist when consumers make payments with plastic cards. Similar to an EMV chip card, a chip embedded in a mobile device, such as the one using a near-field-communication (NFC) chip, can enable dynamic authentication, in which data unique to each transaction is used to authenticate the payer and the payment device. Two prominent mobile payment platforms, Google Wallet and Apple Pay, are NFC-based platforms.³⁴

Mobile payment platforms also use a token to replace sensitive data such as a payment card number or a bank account number. Both Google Wallet and Apple Pay use a token to replace the card number of the payment card to which the mobile payment application is linked. When merchants receive payment instructions from these mobile payment applications, they do not see the card number. Google Wallet generates its tokens in the

“cloud,” in other words tokens are generated at Google’s servers, requiring the phone to have a working data connection to make a transaction at a POS terminal. Apple Pay, in contrast, uses a locally generated token and the token along with other information about the card is stored in a secure element of the mobile device.³⁵ Locally generated tokens are perceived to be more secure than tokens in the cloud, but both types are huge leaps in terms of security when compared to protocols that transmit actual card numbers. Another mobile payment platform, CurrentC, owned by a consortium of many leading merchants called Merchant Customer Exchange (MCX), is in pilot stage.³⁶ Instead of using payment cards and NFC, CurrentC will use ACH by linking a customer’s bank account to its mobile wallet and use a quick response (QR) code to transmit payment instruction from the mobile device to the POS terminal. A customer’s bank account information will be stored in CurrentC’s cloud vault and will not be transmitted to the merchant in the QR code.

To realize security improvements that will be brought by mobile payments, widespread adoption of mobile wallet applications by various types of entities—including consumers, merchants, financial institutions, card networks, mobile carriers, device manufacturers, and technology and payment vendors—is needed. To date, however, mobile payment platforms, even prominent ones, have not gained traction.

When Google Wallet launched in 2011, its business model was murky. Google did not generate fee revenue from merchants and users for participation or for each transaction they received or made.³⁷ Instead, Google experimented with selling ads on the platform and those ads or “offers” were tailored to Google’s existing customer profile. Google collects various data associated with transactions made with Google Wallet.³⁸ Google can use these data, in accordance with Google’s privacy policy, to serve more targeted ads and thereby enhance Google’s core business; however, thus far, there is scant evidence that Google has implemented this practice.

Google Wallet’s business model did not attract card issuers and mobile carriers until very recently. Card issuing banks were reticent to participate, with only Citibank doing so initially. This may be because Google’s weak privacy of transactions did not align well with banks’ long-held norms of respecting customer privacy. As of May 2015, however, Google Wallet works with most major U.S. credit card brands, as well as debit cards and bank accounts. The lack of initial support by mobile carriers, except Sprint, may have been partly due to the lack of fees charged to users or of additional fees charged

to merchants for each transaction. This “no-fee” model conflicted with the business model mobile carriers envisioned, in which a small fee was charged for each phone-enabled payment. Recently, however, Google acquired technology from Softcard, the mobile payment platform jointly owned by three major U.S. mobile carriers, and these carriers agreed to install Google Wallet on their devices.

In 2014, Apple introduced Apple Pay, its own proprietary payment service. Apple Pay uses the same fee structure as payment cards to which Apple Pay is linked. A part of the fee the card issuer receives from the merchant of a transaction using Apple Pay is shared with Apple.³⁹ Other features, including security features, of Apple Pay may reflect Apple’s business model, which is to sell more iPhones. Apple Pay only works on the latest-generation phones (iPhone 6). Apple has chosen to implement a proprietary protocol, as it is not interested in network effects beyond its own customers. As mentioned above, the credential of payment cards to which Apple Pay is linked is stored in a secure element of the iPhone, which is not transferable to another phone. Unlike Google, Apple emphasizes the privacy of transactions—neither Apple nor the merchant can link payments to particular users.

Apple Pay has received much broader initial support than Google Wallet. Many issuers offered support from the time of launch. This may be partly due to Apple’s customer profile—the large number of high-value customers—and partly due to improved privacy compared to Google Wallet. Apple Pay is also supported by all four major U.S. mobile carriers, because they support any iPhone.

Unlike financial institutions or mobile carriers, merchants are not necessarily enthusiastic about NFC-based mobile payments (Hayashi and Bradford). Merchants who plan to adopt EMV can accept NFC-based mobile payments by installing contactless card readers, but for merchants who do not have such a plan, installing NFC-based terminals would be a significant burden. Further, accepting mobile payments that have the same fee structure as payment cards will not help merchants control payment acceptance cost. Merchants also are concerned about ownership and control of customer data captured by third-party mobile payment providers, such as Google. Many merchants expect mobile payments to enhance their ability to collect customer data and engage in highly targeted marketing, but Apple Pay does not enable merchants to do so.

CurrentC's business model is designed to suit the needs of merchants who participate in the MCX. CurrentC uses a QR code to transmit a payment instruction and many merchants may already have QR code scanners in place at their points of sale. CurrentC is linked to customers' bank accounts to use ACH for payments, which are less costly than credit and debit cards for merchants to accept. Using ACH also eliminates the need for financial institutions to participate in the platform. CurrentC can collect information about transactions, which enables merchants to observe multiple transactions by the same customers, as they can currently do with credit and debit cards. Although privacy of transactions for CurrentC may be weaker than that for Apple Pay, consumers who use CurrentC will retain considerable control to limit what information is shared and with whom.

Although CurrentC may have advantage over Google Wallet or Apple Pay in terms of adoption by merchants, it faces the same barrier as the other two platforms: consumers must adopt their mobile payment applications for the platforms to succeed. However, U.S. consumers' incentives to adopt mobile payments seem weak (Crowe et al.). Stronger security and more targeted marketing and rewards offered by mobile payments may potentially entice some consumers to switch from incumbent payment methods to mobile payments (Hayashi). These early adopters could facilitate further adoption if there is a large-scale positive network effect but competition among mobile payment platforms may prevent that.

Mobile payment platforms that compete for market share may not be willing to make their platforms interoperable. While both Google Wallet and Apple Pay rely on similar hardware and have adopted roughly similar technical approaches, they remain mutually incompatible. Competition for the market may undercut the positive network effects and a potential end result could be that no platform gains traction. This, in turn, could inhibit the market for more secure payments from emerging at all.

Consumers' adoption of mobile payments may significantly deteriorate if mobile payments develop a reputation for being unsafe. While the mobile payment technologies do offer features that clearly improve security, similar to other emerging payment methods, mobile payments may face elevated fraud risk during the initial deployment phase (Braun et al.). These risks often diminish once the payment method is established, but the responsibility is on the operators of mobile payment platforms to be especially vigilant

in rooting out fraud during the rollout and respond rapidly to problems that inevitably arise.

Additional vulnerability in mobile payment platforms are new stakeholders, such as device makers and mobile carriers: they do not have the same experience managing operational risk in payments as other existing stakeholders, such as banks and card networks. Shortly after its launch, Apple Pay experienced a huge spike in fraud, in which groups of criminals enrolled stolen payment cards and then used Apple Pay to make large purchases.⁴⁰ Criminals systematically exploited insufficient safeguards in the process some card issuers used to enroll cards into Apple Pay. While one cannot conclude the spike in fraud was due to Apple's inexperience in the payments system, Apple was slow to react to the fraud and did not engage with the issuers to resolve the problem quickly. Apple's reaction may also reflect the fact that card issuers, not Apple, had to absorb the loss on the fraudulent payments. Apple's delayed response may indicate Apple either reacted narrowly to fraud liability incentives or, more plausibly, did not sufficiently understand the elevated risk associated with a new payment product.

Realizing security improvements from the introduction of new payment methods is likely to be more challenging than improving security in the existing payment methods. The former requires additional coordination: adoption of the new payment methods by end-users. Adoption by consumers may be especially difficult and security improvement is not often sufficient to compel consumers to shift from incumbent payment methods to new, more secure payment methods.

IV.iv Cryptocurrencies as an alternative method of payment

Cryptocurrencies is another emerging payment method that offers some promise of enhanced payment security. They offer stronger authentication of payers and payees as well as strong protection against alteration of payment messages and records. But, operational integrity is still largely uncertain. Cryptocurrencies also have potential to attract end-users: a low transaction cost and irrevocability are especially attractive to merchants. However, attracting consumers is more challenging.

Most cryptocurrencies have been designed by those outside of the financial industry, seeking to bypass much of the existing payments infrastructure. Cryptocurrencies have been proposed in various forms since the

1980s, yet none has received widespread interest and adoption until Bitcoin arrived on the scene in 2009 with a mysteriously-authored white paper (Nakamoto).⁴¹ Bitcoin is an alternative currency to hard currencies backed by governments. Bitcoin is specified by a protocol, adhering to rules that are enforced in a decentralized manner with no state backing.⁴² Bitcoin has inspired scores of alternative cryptocurrencies, though none has attracted the participation from users that Bitcoin has.⁴³ As of May 2015, the value of bitcoins in circulation was \$3.3 billion.⁴⁴

While many of Bitcoin's backers envision its primary use as an alternative currency operating alongside or even displacing existing currencies, some (especially venture capitalists who have backed startups) have focused on its potential as alternative payment method. The Bitcoin network offers a decentralized system that facilitates global payments where no single entity controls the network. Its operation is governed by rules set by the original white paper and updated by open-source developers working on the core software.

In some respects, cryptocurrencies are much more secure than existing payment methods. There is no sensitive account information transmitted with payments. Observing the payment message provides no advantage to a fraudster. Protocols rely on public-key cryptography, ensuring that money can be spent only once, and that only the holder of the cryptocurrency can spend it. To initiate a payment, the holder of cryptocurrency denotes an amount of the currency and encrypts a message using a private key associated with the holder.

However, as with any emerging technology, there can be considerable operational risks using cryptocurrencies outside of the core technology, such as the means by which they are acquired and held. Most users acquire cryptocurrencies via online currency exchanges, typically by bank transfer—though some do accept payment cards. In the case of Bitcoin, according to one study, 45 percent of Bitcoin currency exchanges later closed (Moore and Christin). Some closures happened as a result of a security breach. For example, Mt. Gox collapsed in early 2014 along with the disappearance of bitcoins valued at \$460 million.⁴⁵ Exchange collapses matter because many users treat the exchanges more like banks than traditional currency exchanges. Out of convenience (and a misperception of better security), many users who buy bitcoins and other cryptocurrencies choose to leave them in accounts at the exchange. In this case, if the exchanges close, they do not have control of the associated private keys and therefore can lose all money stored at the exchange.

Further operational risks involve the theft of privately held cryptocurrencies, or those currencies held at cloud service providers. Because payments are irrevocable, when cryptocurrencies are stolen there is no recourse. Any accidental disclosure of private key information can lead to theft. Also, malware has been deployed to specifically search for private keys associated with various cryptocurrencies. Hence, the security of devices storing the private keys is crucial.

Apart from operational security risks, cryptocurrencies exhibit considerable currency risk, as evident with Bitcoin. The exchange rate of a bitcoin to U.S. dollars or other currencies has fluctuated wildly (and may explain why Bitcoin has attracted widespread media interest). As recently as January 2013, the USD-BTC exchange rate was \$13. It peaked at over \$1,000 per bitcoin in late 2013 and has fluctuated wildly ever since, falling to an exchange rate of \$239 in May 2015.

In theory, cryptocurrencies could entice end-users to shift away from existing payment methods. Although cryptocurrencies offer weak or no consumer protections, their rules are often very favorable to those accepting payments, such as merchants. Payments in most cryptocurrencies do not have any required transaction fee (though a very small voluntary fee is often paid to support entities who verify transactions). Payments with cryptocurrencies are irrevocable by design. In this way, cryptocurrencies are more like cash than payment cards. While this might put off wary consumers, merchants may be attracted by the prospect of no chargebacks. This may be a reason why Bitcoin is currently accepted by e-commerce companies including Overstock and Newegg. Furthermore, some companies facilitate cryptocurrency payments. For example, BitPay offers a service to merchants that makes it very easy to accept payments in bitcoin and charges no transaction fee to participating merchants. As of May 2015, over 60,000 organizations accepted bitcoin payments via BitPay, and their system is configured so that merchants have the option of immediately converting bitcoins into dollars or the currency of their choice.

To date, cryptocurrencies have made more progress in establishing a seamless process in the market for remittances with low fees. They offer users of international payments less costly choice than traditional international payments that carry high fees. For example, BitPesa lets people send money online to Kenya or Tanzania for withdrawal locally through M-PESA, the popular mobile phone-based payment service.⁴⁶ BitPesa charges a 3 percent transaction fee, considerably lower than its competitors.

However, challenges still remain for any cryptocurrency to attract widespread adoption. First, operational risks must be overcome. Unfortunately, solving them could make cryptocurrencies far less attractive to merchants than is currently the case. For example, if transactions became revocable, chargebacks could become a reality. Similarly, transaction fees may need to be introduced to cover the cost of fraud. Second, currency risks must be addressed, especially for Bitcoin. At present, solutions exist to protect merchants from currency risk but corresponding solutions for consumers are not as mature or widely available. For Bitcoin to succeed as a payment method, an end-to-end solution is needed that leverages the Bitcoin network but without requiring either party to hold bitcoin deposits.

The big unresolved issue for Bitcoin or any other cryptocurrencies is that while it has demonstrated a novel use of technology to ensure the integrity of payment information, it has not developed supporting institutions to protect end-to-end security, or the security of the overall ecosystem. Established payment systems, in contrast, have long histories of using a control structure supported by laws, rules, practices and enforcement, to limit operational risk, including fraud risk. The lack of institutional governance in cryptocurrencies is readily apparent in the inability to root out fraud, support a stable infrastructure for exchange and assure consumers that they will remain safe while engaging with the system. The open question is how cryptocurrencies can overcome a legacy of insecurity and build the credibility and confidence needed to attract participation from the broader public.

IV.v Lessons learned from case studies

The four case studies in this section demonstrate that substantial interdependence in modern payments systems poses significant challenges to improving security. Adopting alternative techniques, business practices, or processing options often involves difficult coordination across various types of payment participants, which may make the status quo appear satisfactory.

As discussed in the previous section, the structure of the coordination game can change in a manner that incentivizes payment participants to adhere to a coordinated security improvement effort. Take for example the first case study, 3DS adoption. Some changes can be prompted by policy actions, such as those taken by the Bank of France, while others can arise organically within an industry, such as in the U.K. The Bank of France's success may be due to leadership advantages to promote collaboration. The

Bank of France is a neutral entity and can more easily build trust among payment participants. It has an authoritative voice for societal interests with a perspective beyond the boundaries of the payment industry. With a long-term focus, it can bring salience to options with extended payoffs. By observing these payoffs, other efforts, such as the U.K.'s may follow.

In the second case study the payment card industry created the PCI SSC more than 10 years ago to develop and promote improved methods of securing data. The Council has played a key coordinating role in developing and maintaining the PCI DSS. While the Council, together with the major card brands that enforce PCI DSS, has increased the PCI DSS compliance rates by merchants, data breaches that exposed millions of payment card accounts have occurred in recent years. It is difficult to assess whether the proliferation of breaches were caused by ineffective leadership or exogenous factors, such as the number of endpoints that has expanded rapidly in the last several years. In either case, public policy could help strengthen involved parties' incentives to protect sensitive data. For example, well-designed data breach disclosure laws incent parties to put more efforts into protecting sensitive data (Schuman); and financial institution oversight includes a review of payment operations the bank conducts and methods the bank should have in place to monitor and deter fraud in its payment operation (Federal Financial Institution Examination Council). Public policy could also help induce involved parties to adopt encryption or tokenization, the protocol that complements or substitutes the protocols of protecting sensitive data.

The third case study, mobile payments, offers a leap-ahead technology. If implemented carefully and adopted widely, mobile payments can substantially enhance security. Apple, Google, and other nonbank payment providers recognize the challenge of adoption by end-users and are taking steps to enhance products to make them more compelling to consumers and merchants. At the same time, added risk comes from multiplying the endpoints and devices where payments are made and from the proliferation of developers with their own mobile payment applications. In the mobile payments space, no entities play the industrywide leadership role to coordinate adoption or ensure security, suggesting a role for public authorities. To that end, the Federal Reserve Banks of Boston and Atlanta have convened the Mobile Payments Industry Workgroup (MPIW) to facilitate discussions among the stakeholders as to how a successful mobile payments system could evolve in the United States.

Cryptocurrencies may be the most vexing of the four case studies. There has been an explosion of cryptocurrency products, yet many do not have a control structure that will reliably ensure their integrity beyond what cryptography protocols can guarantee. In some cases, a control structure is antithetical to the cryptocurrency concept. As other case studies suggest, however, a strong governance mechanism with clear responsibility and authority to implement innovations is critical to ensure system integrity. Public authorities are currently trying to fill this void by working to understand cryptocurrency systems and developing parameters within which cryptocurrency systems may safely operate.⁴⁷ Whether this oversight can balance the need for integrity with the flexibility demanded by cryptocurrency users remains a question.

As each case study suggests, leadership in collaborative efforts is important to appropriately modify the structure of coordination games. Consistent with game theorists' claims, it is observed that the quality of leadership, or the lack thereof, matters (Myerson). Effective leadership requires strong commitment, credibility and understanding conflicts of interests across various parties. These attributes help leaders effectively reconcile the conflicts of interests and facilitate involved parties in building trust. That trust may lead to collaboration on establishing rules or guidelines concerning property rights, distribution of costs and liability, or limited available options to each party. The attributes also help leaders improve involved parties' expectations for prospects and outcomes of collaboration and thereby induce these parties to collaborate effectively.

As history has shown, if participants lose confidence, a payment system can collapse, causing deep economic consequences (Richardson). Some payment systems, such as payment card systems, have grown to be large enough to generate significant disruption from a large security failure. Beyond the payment systems' operators and financial institutions, the economy has a considerable stake in their systems' security. Thus, a strong leadership to coordinate collaborative efforts inside and outside of particular payment systems would be indispensable in providing useful mechanisms that increase incentives to secure payments.

V. Summary and a look ahead

This paper has shown that modern retail payments systems and their security are characterized by several economic principles which make it difficult for markets to reach a socially desirable level of security.

Interdependencies, especially across various parties who participate in electronic payments systems to initiate, process, settle and protect electronic payments, imply potential coordination failure; nevertheless, successful coordination is critical to better protect electronic payments systems.

To understand and help overcome coordination challenges, a game theory approach provides a useful framework. The approach enables us to evaluate if a given game can achieve superior outcomes and if not, to identify sources of conflicts. The approach also helps construct security strategies: payments systems operators and public authorities can use a variety of tools, including liability, pricing, standards and mandates, among others, to change the structures of games so that the equilibrium will shift from a socially inferior outcome to socially superior outcome.

While payment participants put significant individual effort into building strong defenses that contributes to maintaining public confidence, the industry has also made efforts to collaborate to improve retail payments security. When successful, collaborative efforts are often more effective than individual efforts to improve security; however, the four case studies suggest that coordination is a significant challenge. For collaboration to succeed, effective leadership is crucial.

When considering security improvements from a broad and long-term perspective, public authorities may be better suited for leadership roles than private entities. For example, as a neutral, trusted entity, a public authority may be able to spur adoption of security improvement that requires significant up-front investment by certain parties but promises long-term security improvement to society as a whole. Private entities, especially for-profit firms, may not be able to wait for the payoff from a long-term project as their shareholders typically require results in the relatively short term.

Public authorities have become more active in raising concerns over security of payments. For example, in Europe, public authorities took leadership roles in strengthening online payment security, while they also sought collaboration by industry participants. In January 2003, the European Central Bank (ECB) published a report on security of Internet transactions and recommended stronger protections of sensitive data and the use of two-factor authentication for payments initiated via a web browser (ECB). The guidelines on security of Internet payments were initially developed by the European Forum on the Security of Retail Payments (also known as SecuRe Pay), whose membership consists of bank supervisory authorities in the European Union, with significant contributions from payment service

providers. The European Banking Authority (EBA) issued final guidelines based on the ECB recommendations in December 2014 (EBA).⁴⁸

In a similar vein, the Federal Reserve System's Secure Payments Task Force recently engaged a large group of stakeholders with diverse opinions and interests to work toward the common goal of improved payment security. The group's diversity serves the crucial purpose of identifying where strategies to secure payments do not appropriately balance the interests of all payment participants. The Federal Reserve's leadership of the Task Force can contribute a voice for the broad public interest and a long-term perspective on payment security.

While coordination resulting from recommendations of the Task Force can help ensure the integrity of payments, it may require short-term sacrifice from some payments participants. Leadership by a neutral, respected party such as the Federal Reserve may be a key to focusing participant attention on long-term outcomes that will improve confidence in evolving payment systems, ensure that payment innovators can build secure products and ensure that payment participants can safely enjoy leading edge payment technology.

If successful, the collaborative efforts of the Task Force will lead to a more secure and safe payment system. New challenges will nevertheless arise, as they do today, and the payments industry will need to continue to adapt to the changing threat environment.

Time will tell whether the United States can successfully achieve its payments security goals in the longer term with industry collaboration supported by the Federal Reserve exerting a facilitation role. The underlying characteristics of payments that lead to challenges in implementing security may become more important with the continuing shift from paper to electronic payments and the proliferation of endpoints where payments can be accepted and initiated. A longer-term solution may require formal oversight of payment security and integrity, where policymakers can exercise stronger leadership to promote security solutions that are consistent with the long-term needs of all payments participants.

Appendix A: Costs and benefits of 3DS adoption

In the case of 3DS, issuers and merchants weigh costs and benefits while evaluating whether to adopt or not. Table A1 shows the major factors to consider. Both issuers and merchants bear the costs of fixed investments as well as ongoing costs of operations and maintenance. Moreover, a cardholder must be registered with the card issuer to use 3DS, and the checkout process for unregistered cardholders is interrupted for registration, further deterring the customer from completing the purchase. Positive factors include reduced rates of fraud, and for merchants, a lower interchange fee in some cases and a payment guarantee.⁴⁹

Table A1
Evaluating Adoption of 3DS

	Costs	Benefits
Issuer	Fixed investments Ongoing operation and maintenance Lower interchange fees	Fraud reduction Reduction in costs associated with initiating fraud chargebacks
Merchant	Fixed investments Ongoing operation and maintenance Lost sales (first-mover merchants) -higher rates of cart abandonment	Payment guarantee - shift of fraud liability to issuers Lower interchange fees Potential for added sales - more secure card payments adds to consumer confidence in ecommerce and increases online shopping

Source: Adapted from Smart Card Alliance.

Authors' note: Hayashi and Sullivan would like to acknowledge that this paper has benefitted from the Payment Security Landscape study the Federal Reserve Banks undertook to enhance their understanding of end-to-end retail payment security, for which a summary is available at http://qa.fedpaymentsimprovement.org/wp-content/uploads/payment_security_landscape.pdf. The views expressed herein are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of Kansas City or the Federal Reserve System.

Endnotes

¹See Anderson (2001) and Moore (2010) for a more comprehensive treatment of how economics affects information security more broadly.

²Network externalities are also called network effects of demand-side economies of scale.

³Consumers also play a role in protecting payment card data, such as keeping PINs or passwords from being exposed to third parties. Note, however, the role of consumers is limited in that they must accept the technologies that have been offered to them.

⁴The PCI SSC was formed in 2006. For more details, consult <https://www.pcisecuritystandards.org>.

⁵The PCI SSC also establishes and validates security standards for software payment applications and devices into which a cardholder enters a PIN, as well as maintaining lists of qualified security assessors.

⁶However, many vulnerabilities have been uncovered in EMV protocols in countries in which EMV chip cards were adopted. See Anderson and Murdoch (2014) for an overview of the technical literature on weaknesses in EMV.

⁷With this method of tokenization, the authorization request message for a card payment is initiated with a token instead of with the actual card number. The message with a token is sent to a vault service provider, which identifies the card number that corresponds to the token and routes the message to the appropriate card issuer through the appropriate card network.

⁸Akerlof (1970) described information asymmetry between sellers and buyers in the market for used cars (“the market for lemons”). When potential buyers of used cars cannot verify the quality of the cars, sellers of good quality used cars will not place their cars on the used car market. This is summarized as “the bad driving out the good” in the market.

⁹This rationality assumption can be relaxed and more recently the resulting models have been applied to the analysis of observed behavior, including laboratory experiments.

¹⁰A more formal definition is the following: A pair of strategies (s_1^*, s_2^*) satisfies two conditions. First, given Player 2’s strategy s_2^* , Player 1 earns the higher payoff by choosing s_1^* than by choosing any other strategy available to Player 1. Second, given Player 1’s strategy s_1^* , Player 2 earns the higher payoff by choosing s_2^* than by choosing any other strategy available to Player 2. In other words, each player’s belief about the other player’s choices coincides with the actual choices the other player intends to make.

¹¹This example is known as battle of the sexes or conflicting interest coordination.

¹²This example is known as the stag hunt game.

¹³Two main sources for CP fraud are counterfeit and lost or stolen cards.

¹⁴Liability shift for transactions at automated fuel dispensers will be in October 2017. Visa will shift liability of counterfeit fraud, while MasterCard will shift liability of both counterfeit and lost or stolen fraud.

¹⁵MasterCard introduced a security hierarchy in which fraud liability will shift to the party with the highest risk environment. In this hierarchy, MasterCard considers an EMV card used with a PIN to be more secure than an EMV card used with a signature.

¹⁶To simplify the model, all issuers are assumed to be homogeneous and make the same choice, and all merchants are also assumed to be homogeneous and make the same choice.

¹⁷The rate is the gross loss of funds charged back to the merchant for fraudulent transactions. The merchant can then recover funds if it successfully challenges the fraudulent status of the transaction. In 2013, merchants reported successfully challenging 41 percent of fraud chargebacks, which implies a net fraud loss rate of 22 basis points on card transactions. The loss rate is roughly twice that found on all CNP debit and credit card transactions for 2012 (Federal Reserve System). In the Federal Reserve's study, CNP transactions include telephone, mail order and automated recurring purchases or bill payments in addition to e-commerce transactions.

¹⁸An unknown portion of these refunds is fraud by someone other than the cardholder (third-party fraud).

¹⁹Financial institutions report that over half of fraud transactions on both PIN and signature debit cards were on counterfeit cards in 2012 (American Bankers Association). The share has risen steadily since 2006.

²⁰Including cards stolen in intercepted mail.

²¹Many issuers of chip cards in the United States will not require a PIN to initiate a payment, and instead may require a signature or other method of authorization. As a consequence, fraud via theft of payment cards (in person, intercepting mail, or other means) will be relatively more attractive to fraudsters and may increase after chip cards are introduced.

²²If false, the claim of a customer who denies making an online purchase is an example of "friendly fraud," which occurs in both online and in-person transactions.

²³Single-use tokens for CNP payment appear to be more common outside the United States. They are used in the United States primarily for authentication when a password is changed.

²⁴Card companies have not reported how many card issuers have deployed 3DS.

²⁵See Appendix A for a detailed discussion about costs and benefits of 3DS adoption for issuers and merchants.

²⁶The cart abandonment rate for France is about 14 percent (OPCS 2013a).

²⁷In this game, the payoffs are set relative to the status quo of merchants not adopting 3DS.

²⁸Some card issuers, however, have shifted liability onto consumers. For example, the terms and conditions of RBS Secure, its 3DS implementation, state that “You understand that you are financially responsible for all uses of RBS Secure.” See https://www.rbssecure.co.uk/rbs/tdsecure/terms_of_use.jsp.

²⁹Academic researchers panned the initial design of 3DS due to poor usability (Murdoch and Anderson). The design ran counter to many of the cues adopted to fight phishing, such as by asking users to input their credentials to unfamiliar websites. The system was also vulnerable to phishing attempts to retrieve user passwords.

³⁰Other methods of obtaining card data include social engineering, phishing emails and installation of skimmers on payment terminals or ATMs.

³¹The organization that assessed Target’s payment software applications prior to their 2013 breach validated compliance in September 2013, yet the hack occurred only two months later. Subsequently, the assessor was required to enter a PCI Council remediation program, which indicates a need to improve their assessment process (Daly).

³²A recent report found that after validating compliance with the PCI DSS, 81 percent of organizations fall out of compliance within a year (Verizon).

³³After the 2013 breach at Target, many card issuers bore the costs of reissuing cards, added customer services, increased fraud losses and possibly loss of customers in the wake of the breach. Many issuers expressed concern that compensation being offered to them by Target in a proposed settlement between MasterCard and Target was too low (Cumming). The settlement did not receive sufficient support from card issuers and negotiations are still ongoing (Sidel).

³⁴In May 2015, Google announced it was splitting its contactless payment platform from its peer-to-peer payment service, branding the former as Android Pay and the latter Google Wallet. This paper refers to the former service under its original Google Wallet name.

³⁵Apple Pay uses the tokenization developed by EMVCo. The token and card account number are stored on a highly secure server called a “vault” provided by the major card networks and processors.

³⁶See <http://mcx.com/>.

³⁷Merchants were charged a regular payment card fee.

³⁸According to the Google Wallet privacy policy, the following transaction information is collected: “Date, time and amount of the transaction, the merchant’s location, a description provided by the seller of the goods or services purchased, any photo you choose to associate with the transaction, the names and email addresses of the seller and buyer (or sender and recipient), the type of payment method used, your description of the reason for the transaction, and the offer associated with the transaction, if any.” See <https://wallet.google.com/legaldocument?family=0.privacynotice>.

³⁹Apple receives 0.15 percent of a purchase on Apple Pay when it links to a credit card.

⁴⁰By one estimate, the incidence of fraud in Apple Pay was \$6 for every \$100 charged, compared to 10 cents per \$100 for CP transaction (Sorkin).

⁴¹Böhme et al. (2015) provides a primer on bitcoin, especially for economists.

⁴²The term Bitcoin is used to denote both the “coins” and the protocol. It is the accepted practice to use Bitcoin (upper case B) to label the protocol, software and community and bitcoin (lower case b) to label the coins themselves.

⁴³Many other cryptocurrencies have built upon the Bitcoin protocol.

⁴⁴<https://blockchain.info.charts/market-cap>.

⁴⁵<http://www.wired.com/2014/03/bitcoin-exchange/>.

⁴⁶<https://www.bitpesa.co>.

⁴⁷<http://www.entrepreneur.com/article/245994>.

⁴⁸The EBA guidelines have the force of law behind them. Further refinement of requirements for security of Internet payments is expected with an upcoming revision to the EU’s Payment Services Directive.

⁴⁹MasterCard sets a lower interchange fee. Visa sets a lower interchange fee on signature debit cards and no-rewards credit cards.

References

- Adyen. 2014. "Adyen Analysis Reveals Worldwide Impact of 3D Secure on Transaction Conversion Rates," Sept. 1, www.adyen.com/home/about-adyen/press-releases/2014/3d-secure-worldwide-impact-conversion.
- Akerlof, George A. 1970. "The Market for "Lemons": Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics*, vol. 83, no. 3, pp. 488-500.
- American Bankers Association. 2013. "Deposit Account Fraud Survey Report."
- Anderson, Ross. 2001. "Why Information Security is Hard—An Economic Perspective," *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*.
- _____, and Steven J. Murdoch. 2014. "EMV: Why Payment Systems Fail," *Communications of the ACM*, vol. 57, no. 6, pp. 24-28.
- Böhme, Rainer, Nicolas Christin, Benjamin Edelman and Tyler Moore. 2015. "Bitcoin: Technology, Economics, and Governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213-38.
- _____, and Tyler Moore. 2010. "The Iterated Weakest Link," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 53-55.
- British Retail Consortium. 2014. "BRC Retail Payments Survey."
- Braun, Michele, Jamie McAndrews, William Roberds and Richard J. Sullivan. 2008. "Understanding Risk Management in Emerging Retail Payments," Federal Reserve Bank of New York, *Economic Policy Review*, vol. 14, no. 2, pp. 137-159.
- Crowe, Marianne, Marc Rysman and Joanna Stavins. 2010. "Mobile Payments at the Retail Point of Sale in the United States: Prospects for Adoption," *Review of Network Economics*, vol. 9, no. 4.
- Cumming, Chris. 2015. "Banks Stuck with 'Not Fair' Target Breach Settlement, Judge Rules," *PaymentsSource*, May 11, www.paymentsource.com/news/regulation-compliance/banks-stuck-with-not-fair-target-breach-settlement-judge-rules-3021303-1.html.
- CyberSource. 2015. "Online Fraud Management Benchmark Study."
- CyberSource U.K. 2012. "U.K. Online Fraud Report."
- Daly, Jim. 2014. "PCI Council Puts Trustwave's Payment-Software Assessment Practice 'In Remediation'," *Digital Transactions*, July 16, www.digitaltransactions.net/news/story/4773.
- David, Paul A., and Shane Greenstein. 1990. "The Economics of Compatibility Standards: An Introduction to Recent Research," *Economics of Innovation and New Technology*, vol.1, pp. 3-41.
- European Banking Authority. 2014. "Final Guidelines on the Security of Internet Payments," December.
- European Central Bank. 2013. "Recommendations for the Security of Internet Payments," January.
- Federal Financial Institution Examination Council. 2010. "Retail Payment Systems," ihandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf.

- Federal Reserve System. 2014. "The 2013 Federal Reserve Payments Study." July.
- Financial Fraud Action. 2011. "Fraud the Facts."
- Greenstein, Shane, and Victor Stango. 2007. "Introduction," in S. Greenstein and V. Stango, eds., *Standards and Public Policy*. Cambridge: Cambridge University Press.
- Hayashi, Fumiko. 2012. "Mobile Payments: What's in It for Consumers?" Federal Reserve Bank of Kansas City, *Economic Review*, vol. 97, no. 1, pp. 35-66.
- _____, and Terri Bradford. 2014. "Mobile Payments: Merchants' Perspectives," Federal Reserve Bank of Kansas City, *Economic Review*, vol. 99, no. 2, pp. 33-58.
- Heun, David. 2015. "Issuers' Fraud Concerns Undermine Innovation for Merchants," *Payments Source*, May 6.
- Levitin, Adam J. 2010. "Private Disordering? Payment Card Fraud Liability Rules," *Brooklyn Journal of Corporate Finance and Commercial Law*, vol. 5, pp. 1-48.
- Lucas, Peter. 2011. "Canada Puts Down Chip Card Roots," *Digital Transactions*, June 1, digitaltransactions.net/news/story/3176.
- McAdams, Richard H. 2009. "Beyond the Prisoners' Dilemma: Coordination, Game Theory, and Law," *Southern California Law Review*, vol. 82, pp. 209-258.
- Montague, David. 2013. "Finally an Option to Implement 3-D Secure That Actually Makes Sense," March 18, fraudpractice.com/PressRelease-3DS-ImplementationThatMakesSense.html.
- Moore, Tyler. 2010. "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection*, vol. 3, issues 3-4, pp. 103-117.
- _____, and Nicolas Christin. 2013. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk," in *Financial Cryptography and Data Security*, vol. 7859 of *Lecture Notes in Computer Science*, pp. 25-33. Springer.
- Murdoch, Steven, and Ross Anderson. 2010. "Verified by Visa and MasterCard SecureCode: Or, How Not to Design Authentication," in *Financial Cryptography and Data Security*, vol. 6052 of *Lecture Notes in Computer Science*, pp. 363-342. Springer.
- Myerson, Roger B. 2009. "Learning from Schelling's *Strategy of Conflict*," *Journal of Economic Literature*, vol. 47, no. 4, pp. 1109-1125.
- Nakamoto, Satoshi. 2009. "Bitcoin: A Peer-to-Peer Electronic Cash System," <https://bitcoin.org/bitcoin.pdf>.
- OPCS. 2013a. "Stocktaking of Strong Cardholder Authentication Techniques," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 11-14.
- _____. 2013b. "Taking Stock of Measures to Protect Internet Card Payments," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 29-34.
- _____. 2010. "A Stocktaking of Measures to Protect Online Card Payments," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 33-39.
- _____. 2009. "Cardholder Perceptions of Payment Card Security," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 43-54.

- _____. 2008a. "Fraud Statistics for 2008," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 17-26.
- _____. 2008b. "Security Solutions for Card-Not-Present Payments," *Annual Report of the Observatory for Payment Card Security*, Bank of France, pp. 27-30.
- Richardson, Gary. 2007. "Categories and Causes of Bank Distress During the Great Depression, 1929-1933: The Illiquidity versus Insolvency Debate Revisited," *Explorations in Economic History*, 44, pp. 588-607.
- Risk Based Security. 2015. "Data Breach Quick View: 2014 Data Breach Trends," February.
- Schelling, Thomas C. 2010. "Game Theory: A Practitioner's Approach," *Economics and Philosophy*, vol. 26, pp. 27-46.
- Schuh, Scott, and Joanna Stavins. 2015. "How Do Speed and Security Influence Consumers' Payment Behavior?" Federal Reserve Bank of Boston, *Current Policy Perspectives*, no. 15-1.
- Schuman, Evan. 2014. "One Law to Rule all Data Breaches—But Let's Make It a Real Law," *Computerworld*, May 13, www.computerworld.com/s/article/9248300/Evan_Schuman_One_law_to_rule_all_data_breaches_but_let_s_make_it_a_real_law_?
- Sidel, Robin. 2015. "Three Banks Put Kibosh on Target Pact," *The Wall Street Journal*, June 3, p. C1.
- Smart Card Alliance. 2014. "Card-Not-Present Fraud: A Primer on Trends and Authentication Processes," February.
- Sorkin, Andrew Ross. 2015. "Pointing Fingers in Apple Pay Fraud," *The New York Times*, March 16, p. 1.
- Sullivan, Richard J. 2014. "Controlling Security Risk and Fraud in Payment Systems," Federal Reserve Bank of Kansas City, *Economic Review*, vol. 99, no. 3, pp. 47-78.
- TSYS. 2013. "EMV is Not Enough: Considerations for Implementing 3D Secure."
- Turocy, Theodore L., and Bernhard von Stengel. 2001. "Game Theory," CDAM Research Report Series, London School of Economics, 2001-09.
- U.K. Office of National Statistics. 2013. "E-commerce and ICT Activity of UK Businesses," www.ons.gov.uk/ons/rell/rdit2/ict-activity-of-uk-businesses/2013/rf-ecom-2013.xls.
- Varian, Hal, R. 1992. *Microeconomics Analysis*, third edition, pp. 259-284. New York, NY: W.W. Norton & Co.
- Verizon. 2015. "PCI Compliance Report."



The Economics of Retail Payments Security

Commentary

Adam Levitin

Thank you very much for inviting me to respond to a really interesting and much needed paper by Fumiko Hayashi, Tyler Moore and Rick Sullivan. I should say as an initial note, there is an irony that this is a session on the economics of payments security, but we have a computer scientist as a co-author and the presenter, and a law professor as the discussant. While I am a law professor, I do practice economics, but without a license. Despite the scale of the transactions involved in payments, payments remain really an understudied area across academia. Payments security, in particular, is pretty much virgin soil. I think that makes this paper Tyler, Fumiko and Rick wrote really important. It is a great foundational paper, and I think it is going to lay the ground for, hopefully, a lot of future work.

Now, I have no bone to pick whatsoever with the paper's basic argument that economics is a useful tool for understanding payments and payments security, and in particular game theory as a method of thinking about the coordination and cooperation problems involved with adopting payments technology. But, like all modeling, game theory is a type of modeling that is built on a number of assumptions. I want to underscore a few assumptions that I think can be a little problematic when applied to payments security. My point here is not to criticize the paper on these assumptions, because all modeling is built on assumptions and necessarily simplifies. But instead, seeing where the game theoretic assumptions do not hold up is very valuable because it points to where some of the challenges are in payments security.

Let me start by going through what some of the assumptions are that I think are a bit problematic. The first assumption is what I term the "knowledge assumption." This is an assumption that the parties in a game know

how the game works and what the outcomes are, implying that the parties are able to choose rationally between choices such as whether to adopt EMV or not adopt EMV. The second assumption is what I call “causative assumption.” This is often termed as a rationality assumption, but I do not think it is quite that, as I will explain later. The third assumption is “bilateral game,” which is not formally an assumption in game theory because you can have multilateral games. But very often game theory likes to do simple, very clean models with bilateral games. A problem is in payments it is not just two parties in the room. Another problem is that game theory never accounts for externalities or spillover effects on parties that are not involved in the game. If you are thinking about, for example, the EMV adoption game, what about the effect on consumers? Although consumers generally bear very little direct pecuniary liability for fraud, there are all kinds of other costs that consumers do bear when there is fraud; the hassle of having to change your automatic bill payments, the hassle of having to get a new card, and so on. The fourth assumption is “binary choice.” You can have games that have more than two choices but that gets much harder to model. Let me go through these assumptions in a little more detail.

Our knowledge assumption is that the players know what the outcome values are, making a game a static model. In the EMV adoption model, for example, if I adopt EMV, my payoff is 1; if I do not adopt it, my payoff is 2. The problem with this assumption is that we are in a dynamic world where the values of adopting a technology are going to change. We are in a world where hackers never rest, and security within a system can be upgraded. EMV is not a static technology, making it much more difficult for parties to know what are going to be the costs and the benefits of adopting the technology. This dynamic nature, I think, tends to push toward stasis because there are always immediate costs, but the benefits are often less clear.

On the causative assumption, game theory assumes players act based on expected game outcomes. This assumption is often expressed as being a rationality issue, but I think the problem here is not rationality but the fact that security is not a standalone product. Financial institutions, merchants and consumers do not buy security; instead, they get a bundled payment product with various features. Their choices are based on that total bundle, not necessarily on security. Google Wallet, Apple Pay and CurrentC were shown in Tyler Moore’s presentation, and for each one of those businesses, security was a feature, but not what was driving those businesses. For instance, Apple was

concerned about selling phones, and if security helps it sell phones, it is going to double down on security. But at a certain point if additional security does not help sell more phones, the added security may not be an interest of its customers, and thus Apple may stop adding security. There is a limit to how much effort businesses want to put into security, I should say.

How about the bilateral game assumption? Game theory usually models games of two players; multiplayer games are harder to model. But you look around the room and you see all kinds of multiplayer coalitions being represented here. Google Wallet, I think, is a nice example where you had MasterCard, Google and Citibank initially as partners. While two-player games always have a stable equilibrium, with possible coalitions in multiplayer games, we do not know if we necessarily have a stable equilibrium within the games. Of more concern, at least to me, is that game theory never accounts for third-party externalities. Let me give you an example of why this is a problem. If we have a data breach at Merchant 1, that can result in fraud losses not just at that merchant, but at other merchants, and also for banks that do not do any business with Merchant 1. The spillover costs to banks are never accounted for within a game theory model (in which players are merchants only, not including banks), yet that is often how we have fraud losses allocated. I think we need to be a little careful about the bilateral game assumption.

Finally, the last assumption is binary choice; cooperate or not. That is how game theory often sees things. Real life is not a binary choice. An alternative to cooperating in one game is often playing a different game, and it is much harder to model a universe where you have multiple simultaneous games going on. In theory, you could try and add things up, but additivity can be a problem.

What is the implication of these limitations on game theory? Game theory works really well to analyze an idealized version of the world. But when we see where the assumptions do not hold up, I think it starts to point us to a payments security agenda of sorts. Obviously, there is not one single correct setting for security for all payments, but I think there are some broader policy principles that we should be pursuing. I am going to emphasize three of them; data about fraud losses, the need for competitive markets and the need for fairness.

The knowledge assumption points to the need for data. If parties do not know what the outcomes are in the game, they cannot make a rational

choice within the game. That says we really need good data on fraud, which are not just fraud rates. We also need to consider things like definitional questions. How do we define fraud losses? You have the direct fraud losses: someone steals my credit card information and buys a TV from Best Buy. There is the cost of the TV. But then there are all kinds of collateral costs. What about the restocking that Best Buy has to do? What if someone has to run a call center, or add employees to a call center? What if there is data breach notification? Figuring out what costs go in is, I think, a part of getting data and hopefully we can standardize it. The causative assumption and the binary choice assumption point to the need for competitive markets, trying to get an efficient outcome in terms of security decisions. The bilateral game assumption points to the need to be concerned about third-party externalities and try and have fairer markets in that sense.

To achieve the goals of data, competitive markets and fairness, we may need different tools. So let us drill down a little deeper about these three goals. Data is important because it helps facilitate efficient outcomes. This is not just about the choices in the primary market, but we can also think about secondary markets. Normally, when we have risk, we like to see secondary markets develop. The secondary markets not only help parties spread risk but also instill market discipline. There is insurance in payments but we do not have very good secondary markets in fraud risk for payments. One could imagine fraud derivatives existing. I would think that the market would want to create it, but you need data for it. The concern about competitive markets is who is making the rules. We have the problem that rules, or the security standards, may not be set based on what is going to be the most efficient or the most secure, but instead based on other considerations like growth. This is a concern particularly in network industries because if you can grow your market share, you get the benefit of network effects and you may be able to shift the costs of doing so on to other parties. Lastly, fairness is, again, the spillover effect.

How are we going to achieve these goals? There are currently three major approaches we see used. There is private ordering, which is just contract. There is what I am going to call hard regulation, which is command and control; “Thou shalt do, thou shalt not do.” And there is soft regulation, which is a pretty big catch-all bucket for various types of niches, guidance, and I would even say litigation enforcement might go in that bucket.

I want to drill down on soft regulation a little more. That includes a convening and coordination role from the government, and we see the Fed starting to do that now with the Faster Payments Task Force, the Secure Payments Task Force and the Atlanta and Boston Fed's Mobile Payments Industry Working Group. There is potentially data collection which can be voluntary or mandatory, but the Fed is not saying to businesses that they have to adopt a standard or not do something. The data collection is so critical because it allows empirical research and the potential creation of (secondary) markets. It also starts to actually form a common language—it has its own standard-setting role because if you are reporting data in standardized categories, that is a form of standards setting. There are all kinds of regulatory guidance. Governor Powell mentioned the FFIEC guidance. Regulatory guidance is formally not binding, but it is hard to find a financial institution that is likely to openly say no to guidance. We have antitrust enforcement; it is case specific and it is not a great way of doing industry-wide policy. We even have a provision of public options, although I am not quite sure whether to put it in the soft bucket or something else. The Fed as an operator in the payments system is providing public options in terms of ACH clearing and check clearing. And that competition itself helps to frame the market and shape market standards.

Going back, we see these different approaches appearing in different contexts. We see them appearing in security rules, fraud prevention or mitigation rules and loss allocation rules. Security rules are pretty much all set by private contracts, such as direct bilateral contracts, network rules, collaborative standards like PCI, though PCI is implemented through bilateral contracts. There are different ways that these rules get set within private contracts. We also have lurking in the background things like anti-money laundering, national security, and just kind of general reputational concerns that put some soft pressures on security.

For the fraud loss prevention and mitigation, an approach really has been on the state level and it has been state data breach notification laws. These laws are somewhat of a puzzle. They function in some ways as a type of loss allocation rule in that they impose costly duties on certain parties. It is unclear whether these laws in the end are actually a good thing or not. They may help avert some losses, but they are also very expensive. To the extent that the costs of data breach notification outweigh the losses that are averted because of notifications, these laws are actually

Table 1
Consumer Liability Rules

System	Law	Consumer liability for unauthorized transaction
Credit	TILA/Reg Z	Strict liability, but capped at \$50.
Debit	EFTA/Reg E	Strict liability, but capped at \$50, unless consumer was negligent, then \$500 or unlimited.
ACH	EFTA/Reg E + NACHA Rules	No consumer liability.
Checks	UCC Art. 4	No liability unless negligent.
Cash	Common law	Unlimited liability.

functioning as a penalty and we might want to think about whether that is a sensible approach.

Finally, we get the loss allocation rules. They are really important because, as explained in Tyler's presentation, they start to shape the incentives for adopting security rules. The fraud loss allocation rules are a weird mix of private contracts and public laws. As private ordering, we have the network rules for credit and debit cards and for automated clearinghouse (ACH), and even bilateral checking arrangements which in theory can be private arrangements. But then, UCC Article 4 for the checking system creates some hard rules and the consumer liability rules across the board—the Truth and Lending Act (Reg Z), the Electronic Funds Transfer Act (Reg E)—create hard rules on the consumer side (Table 1). Why does this matter? Tyler reasonably expressed some skepticism about whether we should ever be increasing consumer liability; however, there can be some unintended consequences of exculpating consumers from liability. When we look at the consumer rules, first thing you need to see is they are not consistent across products, and it is hard to give a good explanation for that other than historical development. But at this point, if consumers are using Apple Pay, that means they have their mobile device, their new card, their wallet and their hub. With that hub, consumers may not really be distinguishing very carefully between different payment methods. It seems strange to have different consumer rules that depend on the method. Consumer liability is all over the place: in some systems there is basically no consumer liability, while in other systems there is unlimited liability for the consumer. Generally though, other than for cash, consumers have little or no liability for

unauthorized transactions. That oversimplifies, but I think it is generally correct. That is a rule that protects the player with the least market power. But there are some unintended consequences.

Let us think about faster payments, which can often be less secure payments. There can be a trade-off between speed and security. On a very high level, single factor authentication versus multifactor authentication, unencrypted versus encrypted data. Some merchants want faster payments in order to increase sales. I think what comes to mind is McDonald's adopting contactless payments thinking it was going to speed up the lines at lunch time. Consumers do not care much about marginal differences in payments security because they do not bear the costs, which means the costs of having faster, less secure, payments are not fully internalized by the merchants because some of them go on to consumers. But more importantly, some of them are going to go on to other merchants and banks. So here we have this unintended consequence where we have these essentially consumer protection rules, but they may actually be facilitating the use of less secure payment methods. This is a trade-off we have to address. It is not clear that there is a real great answer for how to do this.

Let me throw out two solutions and you are going to see why neither is very appealing. One solution is to change consumer liability; increase consumer liability for unauthorized transactions with less safe systems. That would start to incentivize consumers to demand safer systems if consumers actually end up being liable. But we have card network zero liability policies and it may not be worthwhile for issuers to pursue putting costs on consumers for small transactions, and thus this solution does not really capture the full spillover problem. Additionally, and most importantly, this solution is really politically difficult. To try and change consumer liability rules I just think is a political nonstarter.

A second possible solution is to mandate minimum security standards across systems, which may include mandatory two-factor authentication, mandatory encryption, and so on. That would start to prevent the uncompensated externalities and allow us to have product safety minimums, just like environmental regulations do. But then there is the huge question of who will set the standards and what should they be? That is going to be a real mess.

That brings me close, but not quite, to the end. When we are thinking about private ordering versus public ordering, we have a set of trade-offs

Table 2
Private Versus Public Trade-offs

	Private ordering	Public ordering
Responsive?	More	Less
Expertise?	More	Less
Accounts for externalities?	No	Potentially
Transparent and open process?	Less	More
Other influences?	Market power	Politics

and I think we need to recognize that neither route is really perfect (Table 2). Private ordering is, not necessarily, but probably more responsive and more expert than public ordering. But private ordering may never account for spillovers on to third parties: the parties that are not at the table may not be protected. Public ordering has the benefit of being able to try and address externalities. It does not always get that right, but at least it is possible. Public ordering tends to be more transparent. But what I think really matters is what other influences are at play in private ordering or public ordering. In private ordering a problem is that market power often affects private ordering. In public ordering, it is politics.

When we think about security standards, mitigation rules and loss allocation rules, we see these trade-offs in effect. The security standards, the security rules are technical issues. It makes a lot of sense to have them done by the more expert and responsive body. But exercise in market power may very well mean that we do not get optimal rules as a result. Similarly, for mitigation rules it makes sense to do through public ordering because we are worried about externalities, and the private ordering is never going to account for that. But we may get inefficient outcomes because the rules are driven by politics. So the data breach notifications may very well be inefficient. But the public sees headlines about data breaches and wants something done, and that is as good of a solution as we have come up with so far in terms of loss mitigation.

The real nub though is the loss allocation rules because they are not just about loss allocation. They are about creating incentives for adopting security standards. I think this is where the rubber hits the road. We know

that there are problems with private ordering in this area. Tyler's paper did a wonderful job of showing this. We know that market power affects the incentives of adopting the best security technologies we can have. That said, it is less clear how well we are able to and how good of a result we get, if we were to move in some way toward some form of public ordering. I think though, simply that we are discussing this at this conference is a sign that we are on the way and moving in that direction.

Two things, I think, are really going to drive payments security. One, the headlines about data breaches are creating legislative and regulatory interest in responding to the problem of getting involved. Two, national security concerns are really going to start driving payments security. This is not just a matter of individual consumers and private business concerns, but there is a systemic concern about national security in this case.

Let me suggest that there is a broad agenda we may want to think about. This is a recap and three points again. Data collection—this would be the easiest and simplest starting point for regulatory intervention in the market. Let us just get some data so we can all know what we are talking about and make some sensible decisions. Having that data will also help the private market. We need better antitrust enforcement, but we need to recognize that antitrust is not a good policy tool. We want our markets to work better, but that alone is not going to get us to the right security solutions. And then, we need to be thinking about the problems of how to reduce externalities without creating unintended consequences and often there are not clear answers to how to do so.

I am really glad to have the opportunity to respond to this really interesting and I think very foundational paper on payments security. I hope that this paper will be the start for a lot of future work in this area.

General Discussion

The Economics of Retail Payments Security

Mr. Moore: Thank you for your comments, Adam, and I do think they nicely built on a lot of what I started. I just have a couple of really quick responses. One is the discussion about spillover effects and externalities. I completely agree that externalities are hugely important in this space, and it is true that game theory does not directly account for third-party externalities and that our models sort of ignore them. But what I will say is that game theory is so helpful in describing the private actors taking the decision: it is true that they do not care if they are causing negative externalities on other parties, and so they are still going to take the decision that privately suits them best. I think where it comes into it is when you are thinking from the public/social optimum, we need to actually have a real conversation about externalities. And if nothing else, the fact that we have such pervasive externalities at play motivates the need for greater public oversight and involvement.

The challenges of moving to this sort of public ordering and having a greater public direction, which you also rightly pointed out, are that it is really difficult to envision public authorities developing a better solution than the private sector. What that really points to is the need to have private sector engagement in this, but there is still a role for the public sector to help shape and coordinate the response.

On the point about data, I completely agree, and I think data on fraud can be very helpful in mitigating these key information asymmetries. Many other countries are already collecting data on payment fraud and also security in general. I think it is a key to actually improving the long-run security of our system. It is also potentially less controversial because you are counting things and not prescribing action.

As for an aside point—your question about insurance—cyberinsurance is something that might arise as a result of collecting better data. We have seen this come true in the case of data breaches in that data breach legislation is a very decentralized/indirect way of forcing data collection because you are waiting for the bad event to happen, and now information is being published. But the fact that has happened has engendered a very growing and important cyberinsurance market for insuring against data breaches. I think we could expect to see them. If we start collecting better data and publishing the data, which are also related to other security threats including payments security, it would probably work better. One anecdote: I have talked to many cyberinsurance underwriters, and you are wondering how do they price this stuff? The best I have heard is that the underwriters get on the phone with the security teams at organizations and get a sense of how good a job they are doing and they pull a price out of the air. It certainly is something that could be improved if we had better data on the problem.

Regarding the discussion about consumer liability, I agree the lack of consumer liability can have some of the consequences you have described, but from other research into cybersecurity in general, the direct losses that have been attributed to cybercriminals tend to be dwarfed by the indirect costs related to negative changes in consumer behavior. What I really worry about is that if we increase consumer liability it will shift behavior in a way that is net harmful to the economy by having less engagement in new technologies.

Mr. Levitin: I find cyberinsurance really interesting because one thing we have seen in other markets is that insurers will start to drive practices, levels of care, everything from building codes. Casualty insurers are concerned about having buildings that are less likely to burn down. Life insurers are concerned about people using seat belts. Do you know of anything like that in the cyberinsurance market where insurers are pushing for better practices?

Mr. Moore: This is the great big hope for cyberinsurance. The Department of Homeland Security has been pushing for greater availability of cyberinsurance, hoping this will happen. I have yet to see many examples. There have been informal conversations between underwriters, but the sophistication is not there yet in identifying key controls. But I will say that sometimes they run checklists. If you are not adopting very standard security controls like the SANS 20 Critical Controls, if you cannot show you have taken some baseline measures, then they set a higher price. It is starting to happen, but it is still at very early stages.

Mr. Dubbert: Let us open the discussion to questions from the audience for Tyler, or Adam, or both.

Mr. Grover: Tyler, you commented that Bitcoin was more secure than existing payments systems. By some estimates, roughly 10 percent of all the bitcoins ever issued have been stolen or lost. There is no 24/7, there is no centralized support, and as a network it lacks critical mass. Given that, beyond illicit use cases, do you have a view whether Bitcoin can or will be a long term, viable retail payment system?

Mr. Moore: Yes, the ecosystem is not secure, which you rightly pointed out. We did a study. And around the time of our study, 45 percent of the currency exchanges in Bitcoin subsequently closed. The currency exchanges in bitcoin are effectively de facto banks and so that is a pretty bad bank failure rate. Many of those failures led to a loss of consumer, customer deposits. So, it is not secure in that respect. When I say it is secure, I mean that the payment itself within the network is quite secure and that if you have your Bitcoin account or Bitcoin address, and if you can maintain the secrecy of the corresponding private key, then it is completely secure. But as we know, if you are running this on your computer and the computer gets malware, then someone can obtain the key. There are a whole host of operational security challenges that would need to be dealt with through greater governance and perhaps changes to how they deal with things like revocability of payments. Whether or not it is going to make a long-run impact, I do not know. There are some encouraging signs in a few areas, including one in the remittance market. If you look at international payments, this is an area that is very expensive for people sending money to their home country, and there is a real opportunity for someone to come in and charge less money. The problem is that people may not be able to overcome the technological challenges of having bitcoins, not to mention the risk of holding them. But there is a company called BitPesa, which hooks up with the existing M-PESA system in Kenya so that people in the West can go to their website, send money, and the payment goes through the Bitcoin network and then is received in Kenya through the M-PESA network. The charge is a transaction fee of 3 percent. That is a concrete use case where I could envision this receiving wider adoption. But whether it could also be used to challenge existing payments, I think for it to be successful, first, consumers should not even know there are bitcoins involved. They should not be holding the bitcoin and they should be able to pay in the currency they actually use. There are some efforts to move toward that,

but nothing on the market is really good yet. But there are people working toward that goal. The broader question is what happens with fraud? How does fraud get resolved? I think that has to be dealt with to get wider adoption.

Mr. Levitin: Eric, let me just add, I think where we may see the real value in Bitcoin is as an alternative clearing method. As an alternative currency it is hard to see Bitcoin being very attractive in developed economies with stable inflation. If you are in Venezuela or Zimbabwe, however, Bitcoin may be a more stable currency. But it is exactly what Tyler was saying; that is basically the clearing mechanism, which could be potentially dealing from the currency function and you could have essentially this open source clearing.

Mr. Moore: And there is some technological innovation with blockchains. So, we have this distributed, pretty secure system for processing payments that potentially could be quite valuable. And that is where a lot of the interest seems to be focusing among venture capitalists.

Mr. Hamilton: Very, very interesting. Two quite different lenses on the economics of payments security. If I can, I want to take you back to the fundamentals. I am trying to get away from the “Bitcoinitis” that many conferences fall prey to now. Back on the fundamentals of payments security, it seems we really need to work on defining our underlying policy goal. We have talked a lot about the motivations of the different parties, but what is it we as a community really ought to be trying to achieve? There is an unstated assumption that it should be zero fraud, but I am not sure that is right. So, what is the right policy goal, and where do you think we should be starting in this journey?

Mr. Levitin: There is an efficient level of fraud, but it is not zero. We want to get to where the marginal cost of fraud, or marginal fraud losses, is equal to the marginal cost of fraud prevention. Again, that is not going to be zero. I do not know exactly where that is, and I think we cannot really figure that out until we have better data. But zero fraud should not be our goal. Instead, it should be whatever the efficient level of fraud would be within the system.

Mr. Moore: And zero fraud means that you could always spend an infinite amount on security and you still would not achieve it. One of the things we could do is facilitate adoption of technologies that make payments secure. It is kind of a dance because you do not want to be prescriptive in saying we need to adopt this technology because that tends to favor

the wrong winner. But you can see most of the credit cards in my wallet are running on this 30-year-old-plus technology that is completely insecure. And I think there is a correct perception that what we need is to try to take advantage of some of the technological improvements to security and get them adopted with the idea being that they could reduce fraud rates, potentially also reduce the incidents of data breach and ultimately the amount of money we spend trying to protect this. Because we have this very valuable data that is now widely distributed across tons of companies, we have to turn around and spend all this money to protect the data, but we are protecting it poorly. I think we need to take a step back and say, well, what we need to do is to find technologies that allow us to eventually reduce the overall amount that we have to spend. But to do that, you have to actually spend some money, change the technology and coordinate on the more secure technologies.

Mr. Butler: First, let me preface my question by saying this is not my exact field of expertise. I want to jump back to ask a question similar to the policy question. I recently saw the update to the National Institute of Standards and Technology (NIST) standards, the Federal Information Processing Standards (FIPS) 201 Compliance update for Personal Identity Verification (PIV) cards and federal IDs, et cetera. I would like to understand why we do not use more of what that standard is for federal practices, more in terms of a broad-based consumer application. So, maybe a layer above; use that standard as a means to facilitate and lock down security in a device like a mobile device or card or whatever it is and being able to expand that to just more than maybe access to something, but also using it as a payment device. Does that make sense?

Mr. Moore: So, the NIST standard you are referring to has to do with identity? Like the chip cards federal agents use?

Mr. Butler: Yes, chip and PIN.

Mr. Moore: Well, there is an effort that NIST led, the NSTIC, the National Strategies for Trusted Identities in Cyberspace. That was an attempt to get broader adoption of greater identity management technologies. But it is interesting in that they have some problems in common with payments: a two-sided market. You need to get identity management providers who can authenticate the users, and you also need to get more subscribers who are going to actually have that. It works in the federal government's case because the identity management provider is the government, and it can say employees have to do it. But as soon as you get it to a much greater

distribution scale, it is much harder to actually require or build up that adoption. Then you are stuck with all the challenges of building up a two-sided market, which can inhibit the adoption.

Ms. Garner: I wanted to come back to Adam's chart of public ordering versus private ordering. If you had to rank these from a public policy perspective, and these are all good items to think about, which one or two are the most important to get the best policy outcomes if we do a side-by-side comparison?

Mr. Levitin: I do not have an answer. The chart just represents my own "druthers" and reflects my own priors. I am particularly concerned about externalities. I do not like them in general. I do not want to smell the smoke from the person in the next apartment. I do not like externalities. That would be my first and foremost concern. One general reason for regulation is to try and address the market failure that you have when you have externalities. But certainly, I think we also need to be concerned about market power. We know we have a system within payments where there are network effects that both amplify market power and create an incentive for parties to try and grow their market share; the system has outsized benefits from larger market share. I think that needs to make us very wary of the outcomes in private ordering. Again, I am not sure we know what to do in terms of a regulatory response, but I think we need to be very skeptical about the optimality of the private market in this space.

Mr. Moore: For public authorities, how to deal with these platforms that have such market power is still being figured out, dating back to Microsoft and interventions taken against them. The economics of IT suggest that across many systems you are going to have these dominant platforms that emerge, and they emerge through competition. And so there is a conflict between that and what we espouse in antitrust law and policy. Antitrust was developed in an age where you did not have information markets, and even though there was market power, it did not emerge in as many places. I do not think regulators have really figured out how to deal with it at this point. But that does not detract from the significance of the challenge.

Mr. Taylor: I have a question for both of you. I am with the National Association of Convenience Stores and Conexus. I run a standards organization. When we talk about PCI and EMVCo, I think the biggest mistake people make is that they are perceived as standard-setting bodies, which they are not. They are specification bodies. A cursory look at the bylaws would tell you they do not have the same accreditation as an American National Standards

Institute (ANSI) organization, or even a NIST would have where you have voting on candidate standards. That being a fact, my question is what value do you see in a true standards body mitigating that market power, which is in the box in the private ordering, that might make private ordering, if it was done through a public standards body, a better alternative?

Mr. Moore: What EMVCo creates are de facto standards. But they currently do not go through the same open process you have in bodies like ANSI and even the Internet Engineering Task Force (IETF), which is a private organization. IETF deals with standardization of Internet communication protocols. And what is interesting there is that it is not facilitated by the government. It is a private organization that still does standard setting. I think what that tells us, first, is that standard setting can be seen as valuable to the private sector, even irrespective of government involvement. But the challenge I think that comes from things like EMVCo and the different de facto standards that come up in the payments security space is that with truly open standards, you get much more outside evaluation prior to deployment. I think this is quite critical for the success of the overall security of the resulting mechanisms that are used. Time and again we see secure protocols and mechanisms deployed outside the standards process that are found after the fact to be insecure. I think moving to a platform that has greater openness could really benefit that by making sure the technologies we deploy are in fact more secure. Now, it could still be done, and I am not saying you have to switch to ANSI to do this. You could just have greater openness and move these platforms to have a lot of the same characteristics you have in standards bodies. I think that would be a good step forward.

Mr. Voormeulen: I would like to share one experience from the Netherlands about this topic. I liked what Adam said to broaden Tyler's presentation on what choices people have. What we see in the Netherlands, for instance, if you look at the retailers, even if they have no direct liabilities, they still have a great interest in security. They like to be paid by debit cards because that is cheaper and has less handling costs than cash. But if people experience fraud, they will turn back to cash payments, and cash is more expensive for retailers and leads to more crime, robberies in shops. That is the interest for the retailers. If you look at the Web shops, they have been really pushing for security because they feel that if consumers have some doubts about the security they will not buy things. Their market will expand if security is at a higher level. And if you look at the banks, I do not know how it is in the United States, but in Europe banks today have a little reputation issue. There are many consumer programs on television about bad experiences with banks,

and the banks are really caring about their reputation. If they can find ways to make payments more secure, whether that is through the Internet or at the point of sale, that increases their reputation. If you bring all those parties together, then you come at what Adam called soft policies, and maybe that is also a solution of what to choose there, private or public ordering. In the Netherlands, the central bank tries to bring together the parties—retailers, banks and consumers. I admit that is easier in a country of less than 20 million people than in the United States. But that really works in the sense that, I think, the externalities are taken more into account, and the problems Tyler sketched in game theory can be overcome so that you can go to the bottom block immediately without problems because you take the common interest, which is that everything becomes more secure. Every party in the game profits from that.

Mr. Moore: I will briefly say one thing to that. It is no coincidence that you have had chip cards adopted in Europe sooner than in the United States, in part because you have a much more consolidated sector, which makes it easier for the central bank to bring together the stakeholders and get everyone in the room to agree that they need to move. It is nice if you can do it.

Mr. Levitin: Beyond that though, at least in some countries, the central bank has the authority over most of the players within the payment space. We lack that in the United States.

Ms. Alter: I have an unlucky colleague who had an experience where he was mugged at gunpoint in his neighborhood in Chicago. Within maybe a month, he also had his debit card compromised and his account basically drained of cash. And the way those two crimes were treated was very different. Of course, one was a police report, and the other really was not. And I am just wondering in the case of having a victim, and I do not know if this was viewed as him being the victim of the payment card being compromised, but if those two were treated similarly, would that have facilitated a little better data collection? To your point about gaining a little bit more information about fraud rates and those types of crimes?

Mr. Moore: I would say that if it is physical crimes, they tend to get reported to the police more often, but there are ways to report online crimes. There is an Internet Crime Complaint Center (IC3), which is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance, but there just is not as much incentive to report these cases.

Mr. Levitin: I grew up in Chicago. I would hope the Chicago police would try, if you can identify the mugger in a lineup or something, that they would try and catch the mugger. But I cannot imagine them trying to track down the cybercriminal. Part of it is just the expertise involved in trying to deal with a cybercrime. To the extent we have any expertise there it is not on the local police level. There is a mismatch there. But your general point that it is all crime, that we need to be thinking this—it is all property crime whether it is at gunpoint or electronic, and that we should be collecting data on it the same way—I think is exactly right.

Mr. Marshall: I have a question. This may be describing the problem we are going to have in the next two or three years, but we are already seeing this. Increasingly in the financial industry, we are using one-time passwords sent via email or phone, and we are finding that email companies and phone companies have significantly less controls than we do in financial services, and the losses we are seeing from those one-time password compromises, there is no financial incentive for the email providers or the phone companies to improve their controls. Do you have any advice on what we should do?

Mr. Moore: Because we are talking about platforms, the largest webmail providers account for a very large share of all email. And working directly with Yahoo, Microsoft and Google can certainly help to improve that security. That is kind of a narrow but unsatisfactory answer.

Mr. Levitin: You may want to think about ways of sending that one-time password that do not involve going through the telecom. One example would be having some sort of RSA token built into the device itself. I remember several years ago seeing a Turkish bank issue a card that had that feature.

Mr. Moore: For example, Google has a one-time password authentication token generator built into an app on smartphones. And that avoids network communications, but obviously then you have to worry about the security of the end-user device. But generally speaking, and certainly in the West, smartphone security is much greater than desktop security.

Mr. Dubbert: Tyler, thank you so much for the co-authoring the work to look at the economics of payments security, and Adam for taking the time to respond to that and give very insightful comments.



Monitoring Payment Fraud: A Key Piece to the Puzzle

Alexandre Stervinou

Today I am going to talk about the responsibilities the central bank of France took on a few years ago to tackle the issues we faced, and still face, with payment card security and fraud. I will give you some history and background, but I also will focus on fraud statistics and the trends we see. Some of the data is confidential. I will try to be careful because the 2014 annual report is not out yet, but will be in a few days. And then last, I will talk about some interventions and recommendations we issued to the various market players, and especially the regulated entities.

First, there definitely was a need for public intervention as we saw it, at least in France. In the 1980s, we had two leading domestic card schemes, competing. They decided to merge and offer a universal card payment to cardholders, to everyone. The effort also was accompanied by a push for card acceptance and some kind of connection with the international schemes like Visa and MasterCard to have more widespread adoption and development of cards as a payment instrument in France. Security has always been perceived as a key development for those card payments, and in the early 1990s we had already adopted chip and PIN. It was not EMV because EMV did not exist as a standard at least. But the underlying technology was quite close. Then we had chip, and we also had PIN for protecting proximity payments. But the problem with any type of standards and security, which was part of the discussions earlier today, is that sometimes security is broken. And those issues were arising in the late 1990s. This attracted media attention. The security of the chips was compromised and a lot of the media and consumer associations turned to the public authorities—especially the central bank—to ask what was happening. But it was not only the central bank, but also police forces and the government. We saw that, and perceived the potential to endanger public confidence in cards. Cards and card payments had been taking off for a long, long time in France, so we

had to do something about it. And it came through the French legislature, which took concrete measures with the Everyday Security Act of 2001. That Act, given the tragic events in the United States, led to many different measures regarding security in France, and also, interestingly enough, that included security measures for payment cards. The central bank's mandate basically was extended to payment instruments. The legislature also asked for the creation of a so-called Observatory for Payment Card Security, ensuring the security of card payments, and involving all stakeholders so that what we saw in the few years before could not happen again.

As a result, and I will talk about those two different things, the central bank got that extensive oversight mission and mandate of payment instruments, covering all types of payment issuers and the whole payment chain—the issuing, administering and outsourcing of means of payments. It not only covers cards, but also credit transfers, direct debits, checks and so on. We have extensive power of off-site and on-site inspections regarding all relevant entities in the payment chain. For example, we have the right and ability to go to technical providers or vendors and ask them for quite interesting information about their systems and what they offer to licensed institutions. The central bank also cooperates with the banking supervisors. We have taken review of annual reports from licensed entities on operational risk and the reports have a dedicated annex for payment instruments, including payment cards. There also are some new actors we have to deal with. The EU Payment Services Directive and the E-Money Directive in Europe introduced new categories of payment service providers. We now have some kind of overarching categorical payment service providers. And those payment institutions and E-Money institutions have to be licensed or sometimes may be exempted by the licensing authorities, which very often are the supervisors. At least this is the case in France. But what the legislature wanted was for us to also be part of the actual licensing process, and we have to develop an official statement on the security of payment services and instruments. This also reflects the earlier discussions; we have some kind of clear intervention with the different regulated entities regarding the payment instruments and their regulations.

Now, for the Observatory for Payment Card Security. It is chaired by the governor of the Banque de France. We have many different members around the table. We have a member of Parliament, a senator, and representatives from all stakeholders, including issuers, acquirers, schemes, merchants, consumer associations and government bodies—the Justice Department, the police forces, the Ministry of Treasury. There is a broad

representation of all stakeholders. There are some confidentiality agreements in place because we have issues with some of the data we collect. And the secretariat is insured by the Banque de France. We have three main missions through the Observatory: Deliberating full statistics is a key element, “knowing the data” as it was said earlier; we also have to ensure technology watch and issue security recommendations to issuers, merchants, and all the different actors in the chain; and we have to closely follow up on those security measures, which are deployed by the various entities, various actors. The Observatory publishes the annual report online, which is also available in English, but first in French.

The Observatory has two main working groups—one on statistics and another on technology watch—linked to our mandate. The composition is made of experts nominated by Observatory members, but we also can ask for extended expertise on specific topics—obviously, we have to be careful about the confidentiality of the exchanges. Regarding the working group on statistics, the main mission was first to define what we call fraud and then to define the different fraud types. This work was carried out in 2002-03. We tried to define the different actors, schemes and issuers, how to categorize fraud, how to rely on technical aspects in the networks in the actual clearing mechanisms, and how to take into account, for example, merchant category codes, or error codes from the payment schemes. There was a lot of background work on defining the fraud types and connecting those fraud categories to the reality of the market’s different entities. The main goal of this group is to follow up annually on the statistics gathered from the card payment schemes themselves.

We now have a focus on two main things. One is 3D Secure, which has been put forward as one of the main mechanisms to secure online card payments, along with strong two-factor authentication. I will talk about that later. Another focus is on contactless payments. We began to see widespread adoption in France and there was some fear about what contactless payments can mean from a fraud and security perspective.

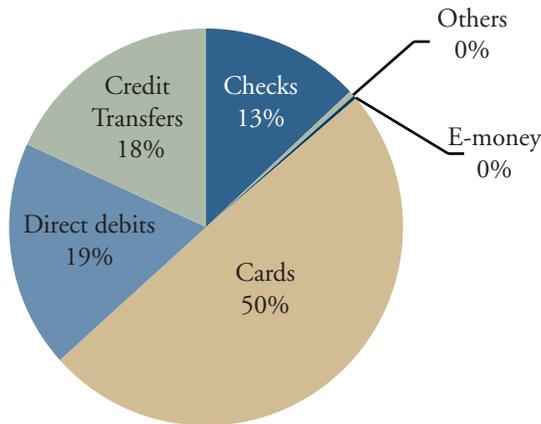
The composition of the technology watch working group is similar to the working group on statistics. Its mission is to maintain a technology watch with the aim of proposing measures to the plenary and its members to increase or maintain the security of card payments. Everything around innovation, mobile payments, contactless, whatever, has to be considered and taken into account within this group. We also have some private or confidential exchanges with a few different actors outside the Observatory membership.

When we talk about technology watch, the Observatory in recent years has looked at different things. For example, we looked at terminals and terminal security. There has been a lot of hype about breaking point-of-sale terminals in the last few years. Regular bus terminals, unattended payment terminals in petrol stations, our networks of connected payment terminals; all of these are security concerns and issues. We looked at that and made extra recommendations. And, in the general topics area, we looked at standardization and certification. This also is a rigorous topic and we need to update our views on this and how things are progressing. With EMV migration, the security of mail and telephone orders and remote payments are things we have to consider; and not only Internet payments. If we secure Internet payments, that means the fraudsters will go to mail order and telephone order. So, we have to look at that and other things. Recently, there has been quite a trend to also look at biometrics as maybe the next step in strong authentication. But today, I will talk mainly about the security of online and card-not-present (CNP) transactions, for which we have gathered statistics in 2008 and 2013, and also about contactless cards, for which statistics have been gathered in 2004, 2007, 2009, 2012 and 2014.

In looking at this annual report and what we do with it, the structure is pretty standardized. We usually have a specific case study that we do as the first chapter. In the last two or three years, we looked at the deployment of strong authentication, and I have a few charts on that. But years before, we also looked at the cost of security and how to compare the cost of security with the cost of fraud. The different market players asked for more data on that, and we tried to run surveys and to have concrete data from banks and merchants regarding the migrations to EMV and the migrations to strong authentication for securing online payments. There also are chapters on statistics and technology watch with the recommendations, and usually a dedicated chapter that has more emphasis on other topics and a little bit more satellite topics or Europeanwide topics. For example, a few years ago there was discussion about the emergence of a European card payment scheme. More recently, it has been the protection of personal data in fraud prevention systems, which raises questions about how you draw the line with problems or issues with data privacy.

I will not say too much about the adoption and publication processes, but basically, the Banque de France is responsible for following up on the recommendations 100 percent of the time. The central bank is doing the work here and using the mandates I explained earlier to follow up on the different recommendations from the Observatory and giving back aggregated information in the annual reports.

Chart 1
Payments in France by Volume, 2014



Source: Banque de France.

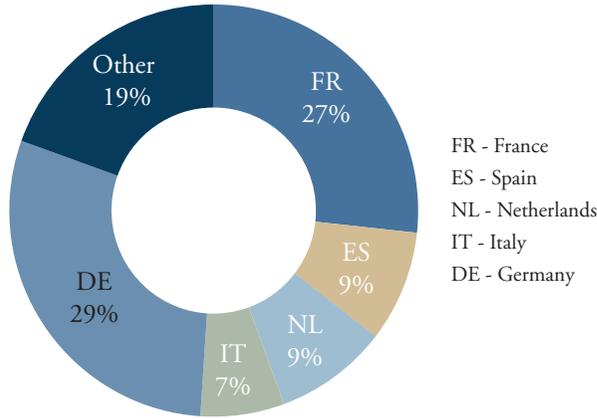
Now to the full statistics and trends. Before going to fraud, I will give you a view on the importance of cards in France. If we look at the volume of transactions in France and the way they split for cashless payments in 2014, cards now account for 50 percent of the number of transactions (Chart 1). So, card payments are already used, convenient, and the main cashless payment instrument in France. If we look also at the weight of the French market in Europe for cashless payments (data are for 2013; 2014 data will be available in September), France accounts for almost 30 percent (Chart 2). So, if you make the calculation, that means we definitely have an important weight just for cards, not only in France, but also in Europe.

Now for the trend we have seen more in the domestic market. Card use is actually increasing, which is the upper line in the chart (Chart 3). Check use is declining; so, less used and less important. For years we more or less have seen the transfer from checks on one side to cards on the other.

All of this leads us to the concrete figures on fraud. We have to follow up on what is happening there. If you look at the value of transactions for cards, we have reached around €600 billion (Chart 4). There is constant growth in the actual value of card-based transactions. So, the amount of fraud is also going up. Even if all cards and transaction types, all are being considered, the fraud rate is pretty stable now, around 0.08 percent. Again, that is considering all cards and transaction types.

Chart 2

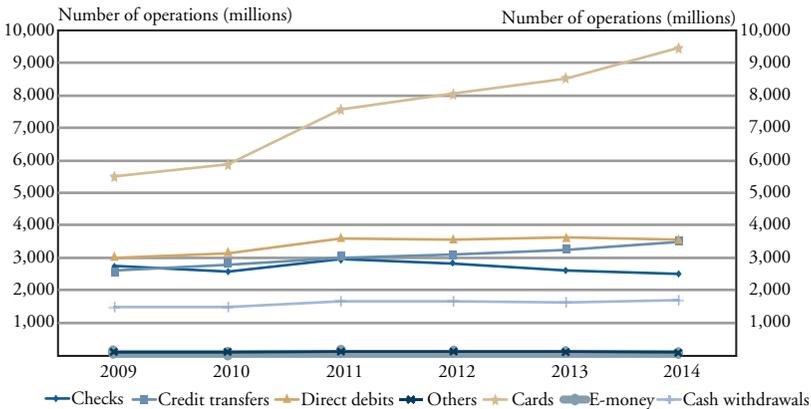
Payments in the Euro Area, 2013



Source: Banque de France.

Chart 3

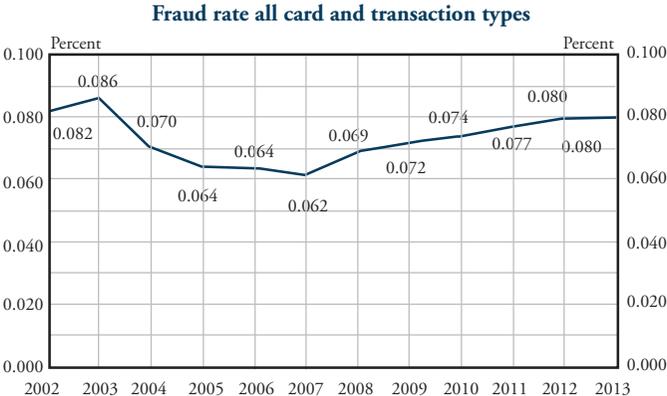
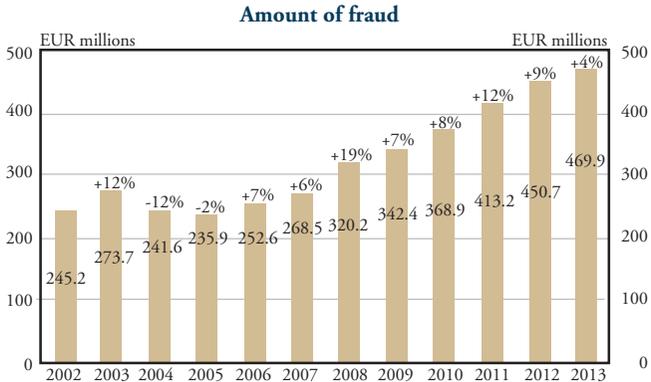
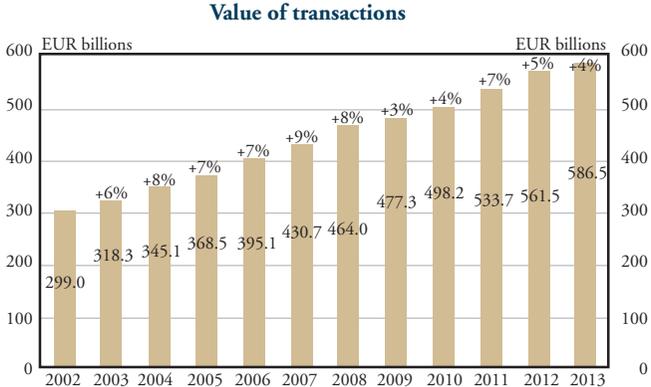
Payments in France by Type, 2009-14



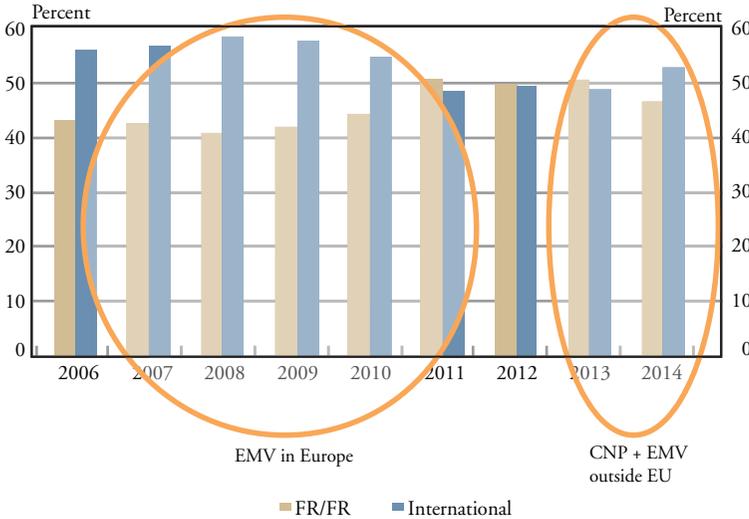
Source: Banque de France.

Now we will look at it in more detail and what all this means because there are huge variations between the territories and the type of transactions. If we first focus on the share of domestic fraud versus international fraud, we already see some differences (Chart 5). The data in brown concerns only domestic fraud and the data in blue is basically everything outside; we have French cards being frauded outside of France and international cards that

Chart 4
Card Payment Landscape in France, 2002-13



Source: Banque de France.

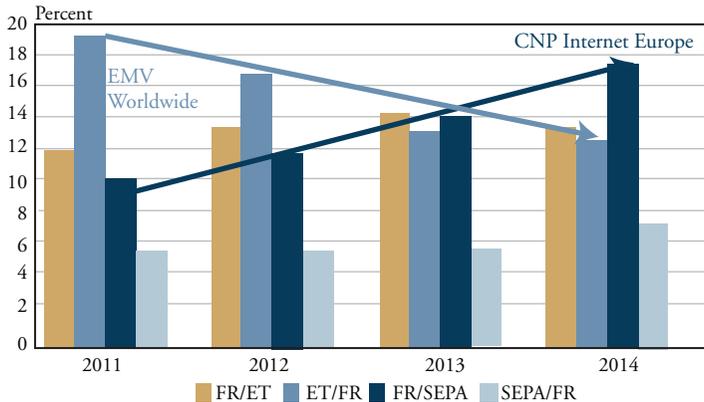
*Chart 5***Share of Fraud in France versus International Fraud, 2006-14**

Source: Banque de France.

can be from the eurozone, the United States or anywhere in the world coming to France to be frauded. So, that is the relative share difference. The domestic fraud share in 2006-08 was quite low compared to the international share. And then we observed that the international share has diminished in recent years, mainly because of the adoption of EMV, after which we saw less proximity-payment driven fraud on the international side of our data. The more recent evolution in 2013 and 2014 is on the right part of the chart, where we see domestic and international diverging again with international fraud increasing. And there are potentially two reasons for that. CNP fraud obviously is still there and very important; and otherwise the adoption or not of EMV outside the European Union.

If we go a little bit further and focus on international fraud only (the blue bars in Chart 5), we have the ability to split this data more, which is quite useful (Chart 6). When we split the data—on one side cards issued in France and frauded in the SEPA or the European zone and beyond, and on the other side cards coming from SEPA or other foreign countries and frauded in France—we see two different trends. First, we see that much of the fraud in the recent years from France has been reported to the SEPA zone, and this is CNP. This would be linked to what I said earlier about the intervention that we have. We took actions to tackle CNP fraud. That fraud then started to deport itself to nearby countries. That is a lesson we

Chart 6
International Fraud in France, 2011-14



Note: Figures are for cards issued in France and frauded in the Single Euro Payments Area (SEPA) and beyond (ET) and for cards from SEPA or beyond and frauded in France.

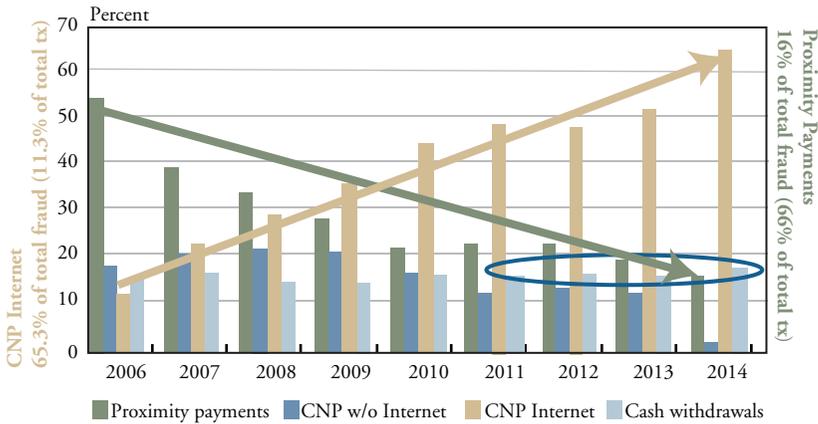
Source: Banque de France.

learned from those figures. Internet-based CNP fraud moved to our close countries. The second thing we can see is related to fraud outside Europe coming to France. We see a downward trend here, and this is the down trend I summarized earlier that we saw in 2006-08. We saw the impact of EMV becoming more positive. When I said international fraud is going up again, this is because when you add up those two different things, you see that CNP fraud is taking over and basically the weight of CNP fraud is much, much higher now than the weight of proximity payment fraud. And this is confirmed by those figures. If the EMV adoption rates could be faster, this down trend would be even better for us and we would see less of that foreign fraud coming to France.

If we focus on domestic fraud, we see two interesting trends (Chart 7). CNP on the Internet has been going up steadily and now is 65 percent of the total fraud but only a little more than 11 percent of the transactions. And the fraud in proximity payments has been going down steadily since 2006, and it is only 16 percent of the total fraud for two-thirds of the total transactions. There definitely is an inverted effect between CNP fraud and proximity payment fraud. We also have a slight concern about the increase we witnessed in the last two to three years for fraud on cash withdrawals. I will come back to this.

If we look at the actual fraud rates for domestic transactions, CNP on the Internet is obviously far higher than anything else (Chart 8, Panel A). And

Chart 7
Domestic Fraud in France by Type, 2006-14

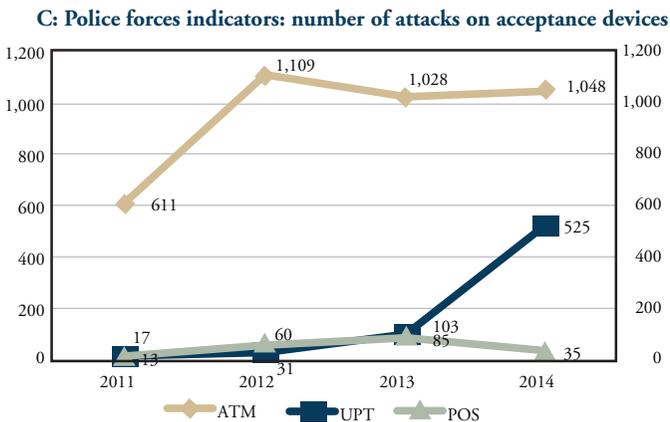
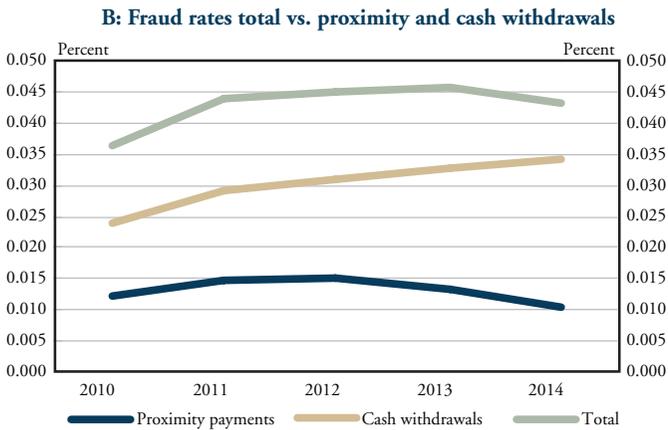
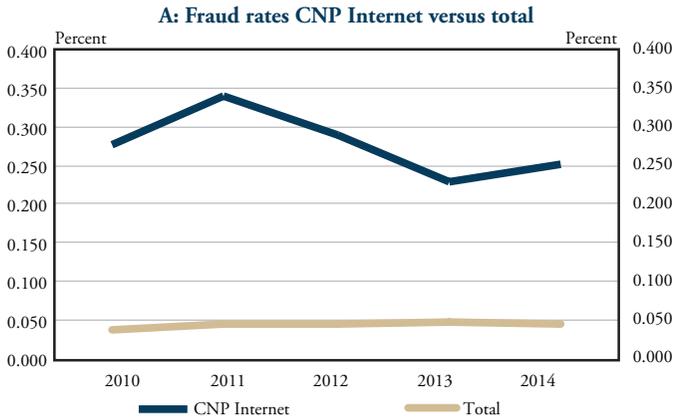


Source: Banque de France.

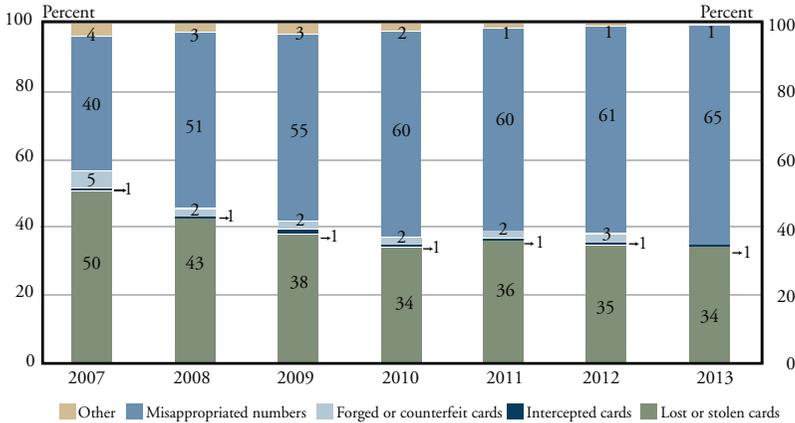
if you compare with the actual total fraud, the total figure for 2014 is 0.043 percent, and CNP Internet is 0.251 percent. That means you have 20 times more CNP fraud than what you have on average. And it is the other way around for proximity payments and cash withdrawals. Proximity payments are very low; cash withdrawals are increased a bit (Chart 8, Panel B). To give us some insights, we obtained indicators from the police forces, the number of attacks on acceptance devices such as ATMs, unattended payment terminals and point-of-sale terminals (Chart 8, Panel C). What you see is that attacks on point-of-sale terminals are quite low. We saw a surge in 2013 due to one terminal being frauded, but not many cases. ATM fraud is still quite significant, and obviously there is a concern. There also is a surge at unattended payment terminals, like at petrol stations. We have to be careful because what you see in proximity payments, even if the trend is going down, someday we may have some concerns about the actual unattended payment terminals and the security associated with those. That is giving us ideas for concrete actions in the next few months or years.

Another interesting thing is to try to determine where the fraud comes from, and the fraud type itself. For domestic transactions, looking at the data since 2007, we see the main two areas where fraud is coming from (Chart 9). The first area is misappropriated numbers, which is basically the numbers fraudsters gather from, for example, card skimming or on e-merchant websites and reuse in online transactions. This is linked to CNP fraud and now accounts for 65 percent of the fraud type origins. The second area is lost and stolen cards. With a lost or stolen card, fraudsters can

Chart 8
Card Payment Fraud



Source: Banque de France.

*Chart 9***Breakdown of French Fraud by Type
(domestic transactions, fraud amount)**

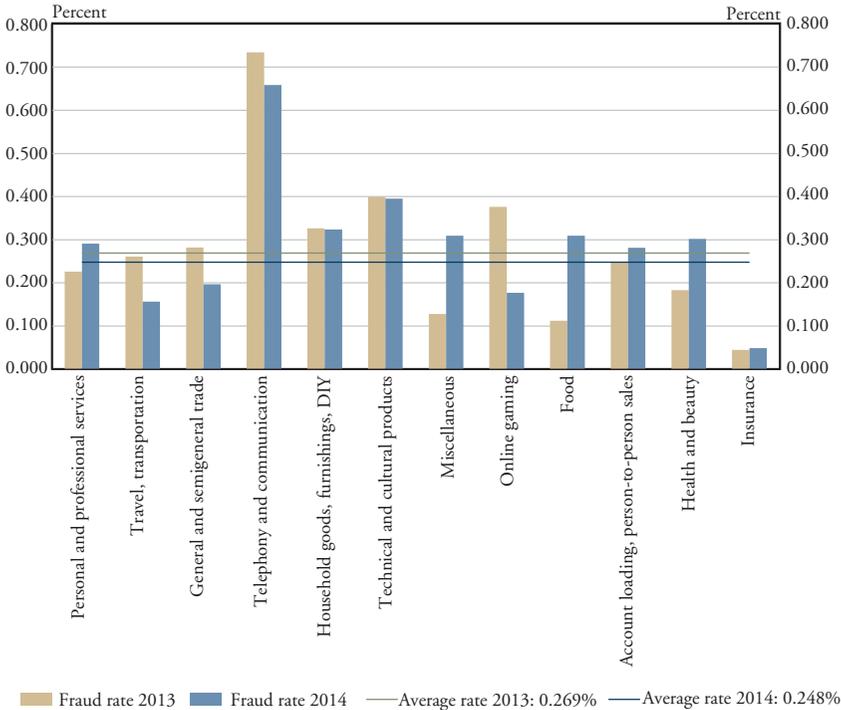
Source: Banque de France.

reuse the numbers and also do some contactless payments. These are the two main trends we see. Anything linked to counterfeit cards has disappeared from the radar screen. In 2007, we had 5 percent of fraud coming from counterfeited cards, but this is not the case in the last few years.

Another thing we do is identify the categories, the sectors where the fraud is being concentrated. We do that on domestic fraud rates and domestic numbers. As depicted in Chart 10, we can see they are always the same type of merchants, which are concerns especially for online card payments and online fraud. Telephony and communication is a main sector of fraud. Pre-paid calling cards, for example, are where the fraudsters are going. So, there is an eye of concern there. Electronics, high technology goods—with online payments—are also where the fraudsters want to go. And online gaming; that was something that developed as soon as there were licenses given to the operators of online games. It was forbidden in France before 2010, and then authorized with a specific license. We saw straightaway a surge in the fraud rates for those online gaming sites, so we took some concrete actions to diminish that fraud and to impose stricter security rules. Now we see that fraud rates are coming back to normal—quite close to the average rate.

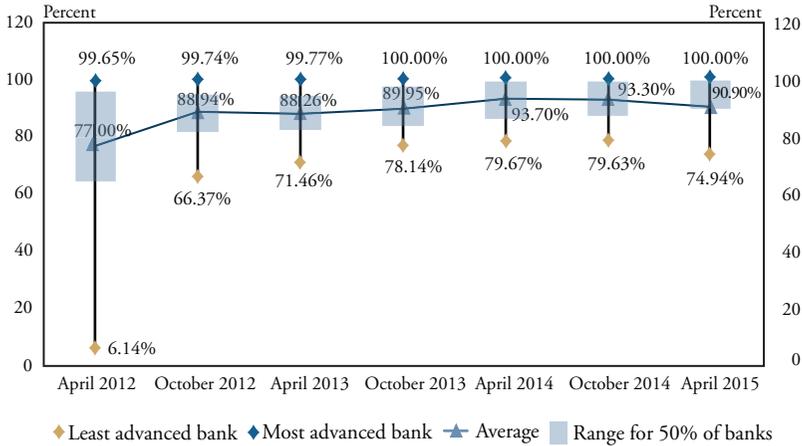
To finish, let us focus on the main security threats we see and recommendations we issued. I will look at what we say about counterfeiting, theft and other areas, focusing on two hot topics in the last two to three years—online identity theft or basically CNP fraud, and contactless

Chart 10
French Fraud Rates for CNP Payments by Sector



Source: Banque de France.

payments. We had to enhance the security of online card payments, based on the fraud figures we saw. The CNP security issue has been the main one since 2008. We pushed for strong customer authentication. We did not push for a specific technology to achieve this goal; we pushed for a level of security. They used 3D Secure, fair enough, but we do not want people to use 3D Secure with static passwords. We want people to use 3D Secure with strong customer authentication—tokens, SMS codes, those types of things. It has been an interesting game. We started first to make sure that the issuers had fully equipped cardholders. So the cardholder indeed has the ability to strongly authenticate when he is making an online card payment. And then we tried to convince merchants that there was a good incentive, like the liability shift, for example, in 3D Secure, to go to strong customer authentication and 3D Secure altogether. To ease the process, we decided to allure them to have a risk-based approach to progressively deploy those technologies at e-merchants at their websites. It is not only a French initia-

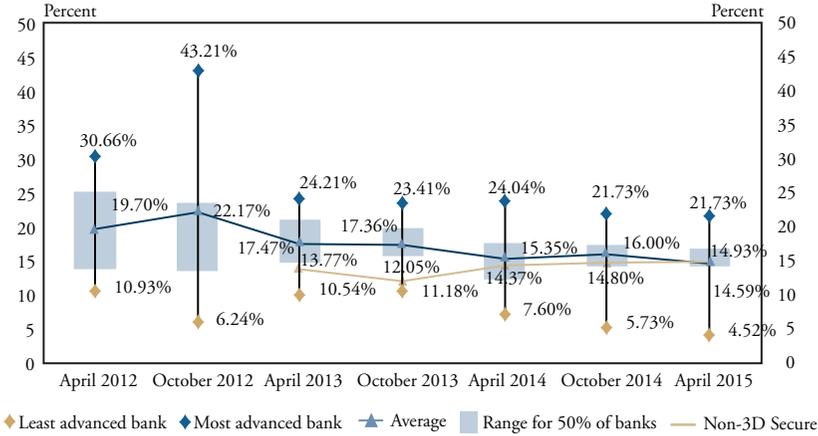
Chart 11**Cardholder Two-factor Authentication Equipment Rate**

Source: Banque de France.

tive, or it cannot be a French-only initiative at this point. If we try to solve the situation in France, that situation will be brought to countries just next to us. So we also strongly supported the emergence of a European initiative on the security of payments and payment instruments, and especially the security of online payments. That is why there is this SecuRe Pay Forum, which was created in 2011. We also tried to push the legislature, at least with the connections we have there, to have more integration of those security concerns within the law. The European Payment Services Directive from 2007 is being revised right now, and will implement strong two-factor authentication in the law, with some kind of a risk-based approach in it. And obviously, we are running data, again, just to understand where we are with all this.

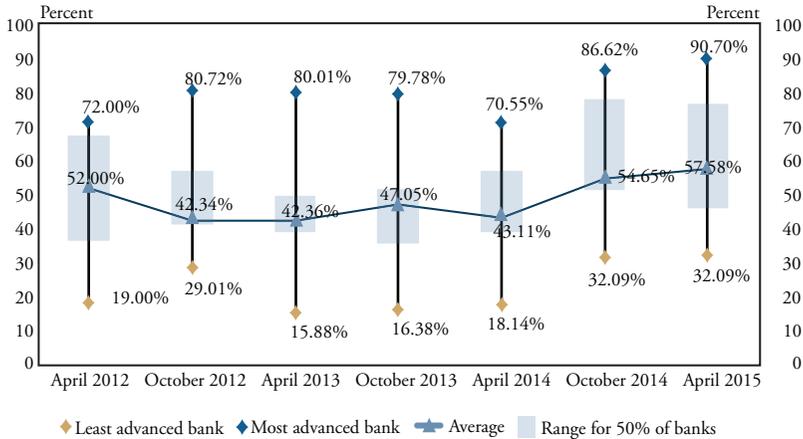
As depicted in Chart 11, cardholders are now fully equipped with strong two-factor authentication. The majority of the banks have a very high adoption rate. Now let us look at the failure rate for 3D Secure, given 3D Secure is the most widely adopted protocol for ensuring the security of online card payments (Chart 12). The merchants have told us they will lose business if they go to 3D Secure. We decided to compare the failure rates of 3D Secure transactions and non-3D Secure transactions. It is very interesting to see that first, there is a large disparity between the different banks on the “crying side.” Some of them have high figures, high failure rates; some of them have low failure rates. But on average, we can see failure rates for 3D Secure and non-3D Secure—these are the two horizontal lines—are getting very,

Chart 12
3D Secure Failure Rates



Source: Banque de France.

Chart 13
E-Merchants 3D Secure Equipment Rate



Source: Banque de France.

very close in the last year and a half. I mean, the failure rate for 3D Secure was down from 17 percent to 16 percent and to 14.5 percent now, which is now about the same as the failure rate for non-3D Secure. So we are convinced, and especially with this risk-based approach in mind, that there is not a compelling counterargument to moving toward those types of secure transactions. That said, we still are developing the adoption of 3D Secure at merchant websites. Right now we see that a little less than 60 percent of the

merchants are fully equipped (Chart 13). That means there is still a long way to go and there are a lot of people still to convince.

Now, I will finish with contactless card payments. It has been a concern since 2007. We have regularly analyzed the lines of contactless technology, looking at threats like remote activation of cards, and eavesdropping on the transactions, so getting the numbers from the cards without the cardholder wanting that. We still conclude that there is more of a reputational risk than a financial one thanks to the transactions thresholds such as the numbers and the amounts of transactions, including cumulative, being there in the cards. And the reuse of the data is actually very, very limited even if fraudsters can still use some of the data on some websites, for example, which is a concern. But we made some new recommendations that issuers have deactivation mechanisms for the contactless interface just in case the technology gets broken at some point. For example, through remote EMV scripts, when you enter your card into an ATM or when you do a proximity payment with an EMV chip, there is the ability to just shut off the NFC communication, so the contactless payment application itself is deactivated. Also, we want the customers to be in control. So if there are fears about that, we ask the banks and the issuers to issue contact-only cards based on customer demands.

For the first time we have fraud figures for contactless payments for 2014, actually for the last nine months of 2014. First, the fraud rate is very close to proximity payments. It is 0.015 percent, which is very low, which is a good sign. Then, a concern was obviously, what is the origin of this fraud? Is it the technology itself being broken by some people? Actually, the origin of fraud is lost and stolen cards, so as I said earlier, if you lose your card or your card is stolen, the fraudsters will get the numbers, go on the Internet, and try to pay with it. But some of the fraudsters also know it is a contactless card, so they usually just go to a merchant somewhere and pass the few transactions they can before the thresholds are met. The data confirms, at least for now, our analysis and conclusions. But we will definitely focus more or continue focusing on contactless payments in the next few years.



Monitoring Payment Fraud: A Key Piece to the Puzzle

Commentary

Chris Hamilton

We are going to change accents now for a little while. First, I am filled with envy for the quality of the material the Observatory collects and publishes. We are still a far cry from that in Australia. It is wonderful to see that kind of quality of data available. I do not want to spend a lot of time on how we do what we do in Australia. In fact, I am going to draw into a statistics presentation without talking about too many statistics. The sheer depth of what Alexandre Stervinou presented to you is a testament to how interesting and potentially useful these data are. But I would really rather talk about the whys and the politics and policy behind this kind of data collection because I think it is more relevant to coming to grips with the public policy implications and what should be done by the industry. Let me start with an anecdote about my past life.

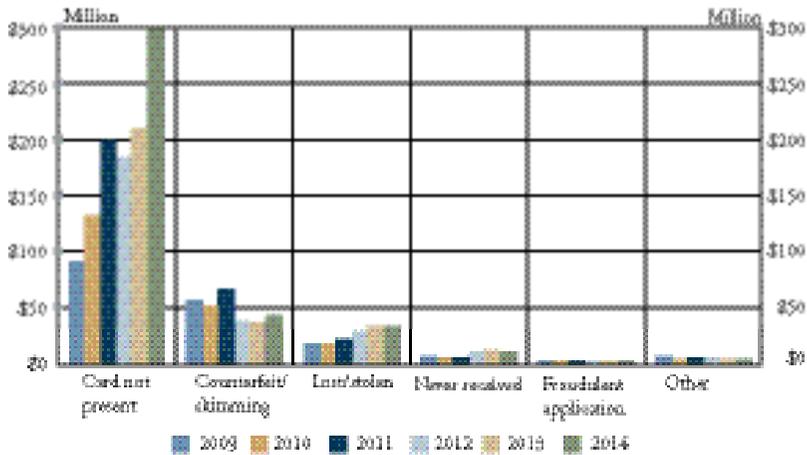
A long time ago, when I was a much younger man, I used to work for the Australian Stock Exchange. You probably know that more than 20 years ago stock exchanges around the world went from being what is called “open outcry,” where everyone yells at each other in a big room, to being electronic, where they all sit at computers and do not talk anymore and just tap the keyboard all day. Some stock exchanges still have a bit of theater around them; the New York Stock Exchange is an example. One of the side effects from going from open outcry to computerized trading is that you go from a situation where the information that is known about the stock market, who is doing what where, the speed of transactions, what stocks are moving, all that is being picked up at the event. If you really want to know it, you have to stand in the room. That is open outcry. We have gone to a world where the entire performance of the stock market is available, down to keystrokes at the hundredth of a second level to anyone who wants it as long as the stock exchange is prepared to give it to them. You go from a situation of quite limited data about what is going on in a very complicated

human environment to where you have almost unlimited data. And that has some very interesting effects on how things are done. This is the analogy I am trying to draw. When the Australian Stock Exchange computerized, which it did relatively early by global standards, insider trading became extremely hard. Although you cannot always tell when it is happening in the market, surveillance experts say an electronic record of trading can always tell you if someone is insider trading because you can see them moving before the announcement. If you have keystrokes down to the hundredth of a second, it does not matter how clever they think they are. You can work it out from the data. What you need is a good surveillance unit that puts two things together—detailed information about trading on the marketplace and key events in a company's history. The trouble with insider trading is that sooner or later the event has to come out, you have to know, and so you catch the crooks that way. One consequence of really good data is a completely different approach to enforcement and quality of law enforcement. But another very important consequence of that change was that a whole academic discipline and tradition grew up around analyzing this volume of data about the trading market to understand how markets work. As we heard this morning, the application of game theory to how stock exchanges work has become an enormous academic growth industry and people understand much more deeply now how markets work because they have this detailed information. There are, however, all sorts of unintended consequences from being able to capture this data, some positive, which are worth bearing in mind.

When I moved to work in payments, about 10 years ago, I felt like I had been blindfolded. We are lousy at data, and we should be ashamed. The quality of detailed data about performance of the payments systems around the world is really lacking and someone should do something about it. The information that we have is after the event. We have publications; I did my publication a couple of weeks ago and Alexandre is doing his in a week. We have data coming out six months after the relevant period. We have relatively high level data about how things work, and we are only able to draw very broad inferences, which we then need to explore further. So, the first thing to say is we should do this a whole lot better than we do, and there is no technological reason why we cannot. As always, it is the human, the economic and social organization part of it that is the challenge.

I want to talk about that. What is it we are trying to capture, and why? Why is that a good idea? Who should capture it, and who benefits from

Chart 1
Australian Card Fraud by Type, 2009-14



Source: Australian Payments Clearing Association.

that capture? Those are the things I want to address, and I will try and draw some reference points from the French experience.

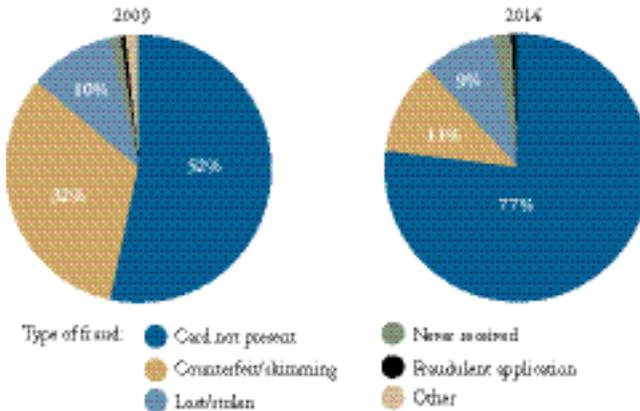
What we want to capture is reasonably clear, and there is an endless further level of detail you can go down to, but the Observatory gives us a very good starting point in terms of what are great things to capture. You want to know about the sheer rate of fraud, the prevalence, and have it broken down in as many different categories as you can. In Australia, we do something similar. We recently published our 2014 numbers (Chart 1). We have been tracking fraud data for about 12 years. This is just a five-year horizon to give you a sense of what is happening, and you can see very starkly the kind of experiences you see in the French data. Card-not-present (CNP) fraud is the big problem of the day. Everything else is nearly solved. It is either flat-lining or dropping. But CNP is the big problem of the age on card data. There is another story elsewhere. Not only is CNP the problem, but offshore CNP is the big problem in Australia (Chart 2). That differs from the French experience just because we probably are on a cycle that lags Europe by a couple of years. I have observed that before, the cycle happening in Europe and then coming to us. That is another good thing to bear in mind as you look at these numbers. And of course, the consequence is, and this is again very similar to the Observatory's experience, over a five-year cycle we have gone from CNP fraud being half the fraud problem to being more than three-quarters (Chart 3).

Chart 2
Card-not-present Fraud in Australia, 2009-14



Source: Australian Payments Clearing Association.

Chart 3
Growth of Card-not-present Fraud in Australia, 2009-14



Source: Australian Payments Clearing Association.

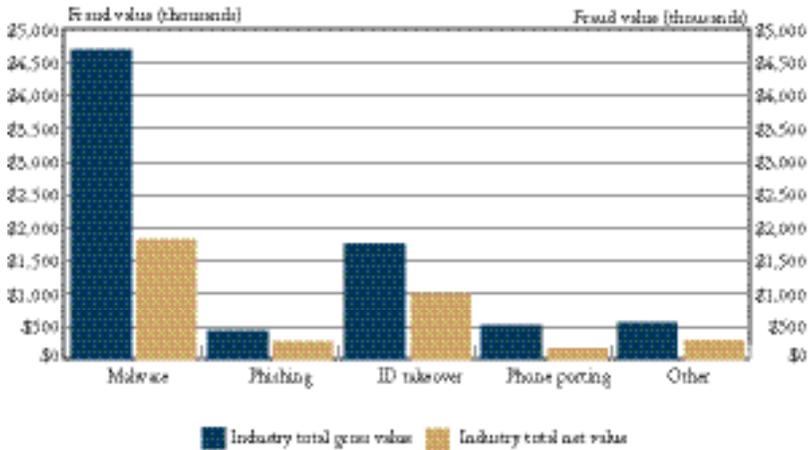
Capturing the prevalence, the trend line, is really important, but it is only the beginning of the challenge. The other thing the Observatory does well, and which we do but in a different way in Australia, is capture the threat matrix to determine the upcoming problem—what Alexandre called the technology watch. In Australia, we do that in a much more informal way, sort of a clearinghouse approach where you get the large organizations involved in comparing notes on fraud events. They take away the raw data of observations and do their own analysis. It is a much more decentralized process. You can argue it is both more and less effective for different purposes. It probably is better if they are looking specifically at protecting their own shops because they will have much more detail on the standing of their own customer environment and their own particular risks and vulnerabilities. On the other hand, it is not very helpful for looking at the global picture and seeing what is happening in a broader sense. One thing that has started in Australia is the formalizing of a longstanding informal structure called the National Fraud Exchange, which is sort of a clearinghouse of ideas. The major participants will all fund and provide threat information and use that as a shared resource across the industry. So, formalizing and automating that process is one of our current priorities.

The third thing, which none of us does very well, but which is actually really important, is impact analysis. What happens when fraud happens? Who actually loses, and what are the costs both of prevention and of the actual event itself? And this is really hazy. We saw some of that in the first series of presentations. Is it really right that the consumer does not bear the fraud? Is it really right that the issuer does? In Australia, officially the issuer bears the fraud, but in practice the great bulk of the fraud is probably borne by merchants because of the various liability shifts. That has very big impacts on their incentives to change and the way they are going to work or not work with the industry. For me, that is the least well-developed of data areas that we should be working on. What are the real costs of this stuff? I am sure the global cost of EMV implementation dwarfs the actual savings in fraud. There is no question that we have all spent a great deal more putting the EMV chips in cards than the fraud that we have saved from doing so. That does not necessarily mean it is a bad idea, but it probably is a useful thing to know. There needs to be much more on that work. If that is what we are trying to collect, then it is worth thinking about the whys. What are we going to do with this when we get it, and who might benefit?

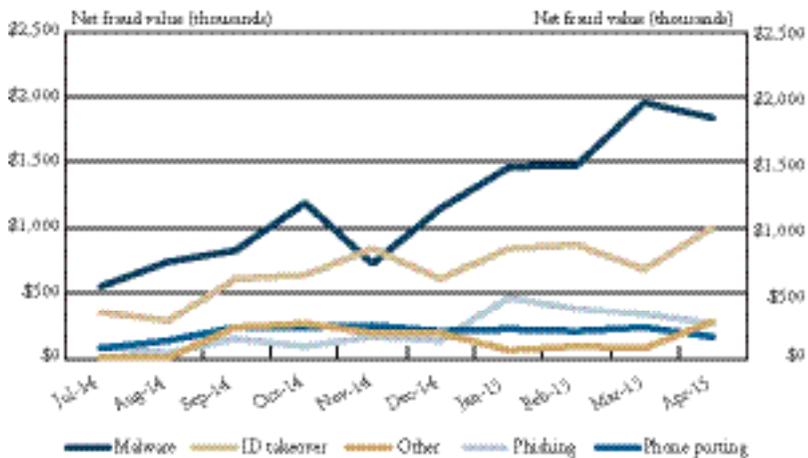
There are several very good reasons. I come at this from an industry perspective. The Observatory thinks about things from a public policy

perspective—what is in the best interest of the community? I am coming at it from a slightly different perspective and I should explain what the Australian Payments Clearing Association (APCA) is. It is not a government body; it is completely privately funded. The nearest equivalent in the United States is the National Automated Clearing House Association (NACHA), but we are not that much like NACHA; APCA is an organization that administers the rule books on behalf of the financial institutions in payments. So, we are only as good as the collaboration we can persuade our members to perform in improving the overall payments system. Our goal is to improve the payments system, but from the industry perspective of how do we work together as a community on what is important to all of us to make the payments system better, rather than what is the public good. Public good clearly comes into it; it is clearly a big factor. But we need to marry that with the collective industry of the community. Coming with that lens to this fraud data, why would you voluntarily publish fraud statistics? In many countries, that does not happen and there appear to be good reasons why. People do not want their brands associated with large reported frauds. People do not want to scare off customers with stories of fraud. But that is a shortsighted view; the much better path is to think about the long-term gain for the industry. So, forget the public good for a second.

The people mostly affected are our collective customers, the consumers and businesses of the community. There is a sort of moral dimension here where they have a right to know so they can do their own risk assessment. That is one reason why it probably is a good idea, but there also is a practical one, which is they need to be participants in the fraud-prevention process. Consumers and businesses all can do fairly basic sensible things to minimize their own risk and prevent fraud. They cannot, however, solve the problem by themselves. There are many other things other people have to do, but it would be nice if they were active participants in that process. You start doing that by educating them about fraud, by giving them a clear picture of what it is (Charts 4, 5). So, that is a good, practical reason for industries to do this work voluntarily. The other obvious benefit relates to a point made before—what gets measured gets managed. Unless we know what the fraud is, we do not know where to focus our limited dollars on trying to prevent it and improve it. It is very important to have that kind of data when you are arguing the case for whether we should do EMV, or go to two-factor authentication or 3D Secure. And not having good quality data is one of the things that makes that process quite hard. In Australia, we had an initial go at EMV, at chip cards, more than 10 years ago; not as far back as the French. That effort

*Chart 4***Gross/Net Fraud Values by Fraud Method, April 2015**

Source: Australian Payments Clearing Association.

*Chart 5***Net Fraud Value by Fraud Method, July 2014-April 2015**

Source: Australian Payments Clearing Association.

failed through lack of articulation or a strong enough case for change. I think if we had had the quality of data and the trend lines we have now about fraud, you might have gotten a different result. Indeed, the second time around, having the benefit of that information was at least as important a factor in what has been a very successful chip conversion.

Having a grip on that helps the industry work out what it should and should not do collectively to improve the system. The data also give organizations a much better risk management capability within their own shops. All large banks around the world now are scoring approaches, doing risk approaches to fraud—some are really good at it and some not so good—but they all would get much better if they all had all the data. Seeing their own data is not enough, and having the benefit of detailed information about data is potentially extremely valuable.

If that is what we are trying to achieve, then the last point I want to cover is who needs to do this, and how they should go about it. And I am going to give a slightly different point of view. I do think that this generally is actually better done by industry. I *would* say that, would I not? I work for industry. Natural bias. And yet, my experience is that work to improve the overall payments system, which is done collaboratively by the institutions that work in it, when they are convinced there is long-term benefit both for their customers and for them, is much better done than forced compliance as a consequence of regulation. It is hard to pull off. It is much harder to do. So, compliance in a way is easier. What happens is the banks have outsourced to the regulator the problem of deciding what should be done because the compliance rules tell them what should be done. They can comply and they get to bellyache about it at the same time—sort of a win/win. But in the long run, these things work a lot better if, having been convinced of the need to actually make the change, they then implement it because they will do it in a cost-effective way. They will do it in a way which fits with their business, but still meets the public policy goals.

The last thing I want to talk about is this Australian way of having a go at the public/private partnership. Let me observe that in relation to Adam Levitin's distinction between public ordering and private ordering, I am suggesting that is a bit of a false dichotomy, or at least it should be. What we really should be doing is finding a way of marrying the public and private methods of doing things, and the public and private interests to get the best possible outcome. And I think that is possible, if you can get the industry convinced of the value to them, which is also in the public interest, you can then get a willing, collaborative approach to solving the problems we are talking about. And in fraud, that actually works better than many other areas of changing the payments system because it is easier to convince people that fraud is everybody's problem. It does not tend to have a major comparative element to it. It sometimes does have little bits of competitive tension among the banks, but in general, people agree that if I am lax on

security it is going to affect you and vice versa, and so it is easier to get that collaborative agreement. My suggestion is that in the long run, we need to gather this data because it is in the interest of the industry. But then we need to work on it together to find the best way of improving the payments system using the data itself.

General Discussion

Monitoring Payment Fraud: A Key Piece to the Puzzle

Mr. Dubbert: Alexandre, would you like to take a couple of minutes to respond and reflect on Chris' commentary?

Mr. Stervinou: I think there are two different things, two different dimensions. The first is everything about the collection of data and the idea of collecting data. The second dimension is how a public authority intervenes in the field of security. And those are two different things. The fact that we as a central bank wanted to intervene in the field of security also pushed for a central bank-led initiative of collecting the data. We had to have this necessary means to get to the ability to issue recommendations. That said, in the U.K. and Australia, there has been this market-led initiative of collecting data, and we see more or less the same trends and more of the same concerns.

Having an authority get involved in collecting the data may be the neutrality of things, which also has been said this morning. Collecting the data must not be a competitive issue. Having a public authority with confidentiality agreements that are mandated will ensure confidentiality. Collecting those data, having the ability then to drill down into details, that may be something market-led initiatives would not be able to do? I do not know. But having this ability helps us get more insights on how fraud is moving, where it moves, and sometimes the cost of it. That also is something we learned to do; ask beyond the fraud figures, ask about the cost of the security measures you are deploying. Again, having the public authority doing this exercise is of benefit to everyone. We have done that with EMV and with two-factor authentication. With EMV, it helped not only the banks but also the merchants to understand a little bit about their fees and the way we are paying for security. The benefit may be realized in the mid- to long-run, not in the short-run, and that was one point in Chris'

presentation. I agreed: in the long-run it actually helps them fight fraud. Showing through a public authority that the investment on EMV was fruitful for them in the long-run is of benefit. Those would be my comments, which are just complements to Chris' presentation.

Now for actual public intervention, I am convinced that this is useful. As Kelly Dubbert and Governor Powell talked about it, we have to find the right balance between the flexibility of having the economy and the market players doing what they want to do and innovate in several fields, and having too much, too strict regulations. In France, regulations have always been quite heavy and quite present. It is becoming more or less the same in Europe; European-led initiatives in regulations and directives are getting stronger and stricter. Is it the right path? I think only the future will tell, but I think it can help at least on issues like security that are definitely of public interest. It can at least help to state the scene and not let market players do things that are not good for them, for consumers, or for their merchants.

Mr. Hamilton: I think we are not so far apart. I would not deny the role and importance of having a public policy regulator, if for no other reason than because the only organization that can prevent what the thinkers in this field often call regulatory capture is the public policymaker. If your self-regulatory system is in fact captured by special interest groups, the public policymaker has to decide when to intervene. One of my colleagues at the Reserve Bank of Australia used to say that it is very important to have a very large club to hit people with, but ideally he never wanted to take it out of the cabinet. I think there is some logic to that. For a long time, the Reserve Bank has had direct and specific regulatory paths over payments in Australia. And I know that it has a global reputation for being quite interventionist because of the interchange fee regulation that it undertook some years ago. But in fact it has used regulation extremely sparingly. It only had to prove that it was prepared to take the club out of the cabinet once, and that has been very, very helpful in engaging industry in a fruitful discussion because the industry would always rather organize to meet the public policy goal itself than be forced to. That certainly is a valuable way to balance the public and private interests, and I think it is going to be a partnership.

Mr. Dubbert: Very good. We will open it up for questions.

Mr. Horwedel: Two questions. First, you had those two slides in the five-year period. What is your view of the allocation of fraud between

issuers and merchants five years ago, and then what is it today? The second question is what is your view of the fact that we are going through this expensive conversion to EMV in the United States without mandating PINs?

Mr. Hamilton: The honest answer to your first question is I do not know because I do not know what the picture looked like five years ago between merchants and issuers. I suspect there probably has been a shift toward merchants over that period. A little bit of background on that: the Reserve Bank of Australia, although it has a lot of power, has never done anything in a regulatory way in relation to fraud prevention in the card system. It has never found the need to. And when you ask them why, they say some version of—and I can say this, but you probably would not get them to say this publicly—as long as the responsibility for fraud is well aligned with the people who bear the consequences of fraud, then we are going to be happy because they will find the right level of fraud prevention. They keep an eye on the relative ability of different players in the marketplace to manage the fraud problem versus actually bearing the costs of the fraud problem. As long as those two things are roughly aligned, their decision is not to intervene. Or at least, that is my observation of their behavior. So if that balancing shifts, it should be because the ability of different parties to prevent the fraud has shifted and that is what things like scheme liability shifts are about. They are trying to say that if you implemented the right security measures, you would be able to prevent this fraud and therefore we are going to allocate some of it to you. That might be right, and it might be wrong, but that is the theory.

Your second point was about the cost of EMV? It is a done deal; it does not matter anymore. The reality is globally the world is going to EMV and even if there was not any fraud cost benefit, you need to do that as a transitional mechanism to get to this. And we are all definitely going to this eventually. That is the way it is.

Mr. Horwedel: My question, though, is going to EMV without PINs.

Mr. Hamilton: OK. Both are useful on their own, but the better configuration is to use chip and PIN. Whether it is better to do one first then the other, I do not know, but presumably that is the path that you are on.

Mr. Stervinou: Regarding the split of fraud between issuers and merchants, this is something we ran and saw as data for a few years, but we decided to stop in 2011. The data were not reliable enough. The issue

we have, and this is also why there is a delay in creating fraud data, is we may have fewer chargebacks due to commercial litigations between merchants and consumers. It takes maybe two or three months to settle the transactions properly. When it comes to the actual split of the fraud cost between the issuers and the merchants, it can take longer than that. It also requires us to know exactly how things happen between the acquirer and the merchant, but that is difficult because the acquirer and the merchant may have agreements that the acquirer is not passing the cost of fraud to the merchant, or is passing it differently in different contractual terms. The last data showed the split was like a 50/50, but if you look in detail it was actually more like 40 percent for the issuers, 40 percent for the merchants and the rest for the cardholders. I would say, with the liability shifts, the split should have evolved to the issuers taking more of the cost of fraud, but I do not know. We do not have concrete data anymore and it is rather difficult to collect.

On your second point, yes, I would agree. Chip is half the way through: It is a good half, but it is still half the way through.

Mr. Santana: You talked about collecting data, disseminating fraud data. We have a unique problem. In our market, at least in the United States, if you look at the card, the share of the card market, the cards in force, you would see the top issuers control maybe over 70 percent. As a result, if you start sharing fraud data, there is a general fear that it only benefits the smaller issuers, and it exposes their card data to merchants and that may have unintended consequences on interchange rates. How did you overcome that problem in Australia and France? We have this ongoing dialogue with issuers and card acquirers and this is their general fear.

Mr. Stervinou: I will take the case of France. We aggregate a lot of the data that we have. Data aggregation gets a lot of the details out of the picture. Our market is made of maybe nine to 10 major banks, and we have probably 100 behind those. Aggregating the statistics and choosing to give only a certain level of information to the market helps address the issue you are underlining.

The fraud data help with another thing, which is also part of your question regarding the actual cost of fraud and the cost of the measures being deployed. For example, seeing CNP fraud being at 25 basis points gives you ideas about the price of security in contracts between the acquirer and the

merchant, which can help in a way because it is how it works in the overall market; it is not with a specific acquirer, but it is with all different banks. I remember one thing I did not talk about. When we wanted the industry to tackle CNP fraud in 2008, we said let us push for strong customer authentication, two-factor authentication. One or two years after that, we realized some of the acquirers were offering 3D Secure to their e-merchants with an additional fraction of merchant fees, which was higher than the cost of fraud. So, how do you work on this? This was part of the presentations this morning regarding what is the right level first of all, and also how do you choose your incentives. With public interest in mind, I think showing that type of measure or that type of statistics helps to have a responsible action or behavior from the banks and from the merchants.

Mr. Hamilton: I agree with that. I think the way in which the Observatory presents the data is very important in answering that question. I would add that it is important to trust who is collecting the data and presenting it because you do need to mask information that is competitively sensitive. We in Australia had quite complicated negotiations with the card schemes, not with the issuers, around their competitive positions. There is a lot of competitive tension between the domestic debit card environment and the international schemes in Australia. Neither wanted the other to know what either their volumes or their fraud experience was. So we need to manage that issue. We need to be trusted as an organization that is able to hold that data and keep it confidential and only present the information which is acceptable. Although there is a negotiation to go on there, the short answer is it should not impede getting the benefit out of the data.

Mr. J. Williams: Adam Levitin said earlier on that one of the key things is sharing data, and as part of that it is the definitions you are using as to what you count as fraud and what you do not count as fraud. There is great potential for unintended consequences to shift what actually is fraud into something you are not currently counting. I think there are some good examples of that. So how important do you think consistency is in our definitions of what fraud is, either across payment mechanisms or between different countries? Because I think it could be a key chink the fraudsters could take advantage of if they can move their fraud to some other mechanism you are not counting at the moment.

Mr. Stervinou: Maybe two aspects on this. If there is fraud, at some point, it will be counted as fraud. So, I do not think the general value

such as overall fraud rate or amount will be different. But what becomes important is to know where the fraud comes from. So, the distinction between proximity payments, ATM withdrawals and then remote payments from mail order, telephone orders and Internet payments becomes more difficult. Defining the fraud types for cards today is not a concern anymore. The problem is that you still need to count correctly the data from the payment chain. I think what the Observatory presents is pretty reliable—we have been dealing with this for 13 years now—but we still have concerns. There are areas where we are not sure. For remote payments, for example, the split between mail and telephone orders on one side and Internet fraud on the other side is still a concern because the data quality itself is a problem. Also, merchants have to be in the right merchant category code. Merchants have to correctly split those transactions between what they do in proximity, in mail order, on the Internet, and so on, which, however, is not always allowed by the systems. The IT systems behind the merchants aggregate transactions too early in the process. The acquirers are trying to convince their merchants to follow the guidelines, but sometimes it is a little bit difficult. I think we are still victims of that, and everyone is, including the card schemes. The card schemes have a global view on all this, but their view is as good as their member banks. So, we have trajectories in place to try to improve this, but it is rather difficult.

To conclude, you said consistency is important. Yes, for sure. Again, I think consistency is achieved because fraud on cards is known for years now. So I do not think there is a big issue in that. In Europe, we are trying to bring that consistency for the figures we are now starting to release on fraud for cards all across Europe. When we worked with the ECB within the Eurosystem, we did not face any stronger issues in having consistency across the figures released by the ECB and our figures. But the issue is definitely still there in data quality and the way the people, the economic agents, report the information back to the authority, the card payment schemes and all associations.

Mr. Hamilton: Absolutely, it is a pain. It is hard work. We have been collecting information on these phone and Internet-based fraud events for a couple of years now. It is not in publishable quality at the moment. Indeed, the only way you can get it there is by collecting it for several years and going back around, testing, retesting, checking it and making it more consistent. The key thing is do not use this as an excuse not to get going because it actually is a process of gradual refinement. But it is kind of interesting because it

does show things like malware is a much bigger problem than phone porting or at least on the data we have. Is that true? I am not really sure yet, but you have to start, and you have to refine the categories as you go along and prove it over time. And I would try and do the international bit last. I think it is probably more important to produce quality data that gets relied on domestically and then try and adapt.

Mr. Moore: I have a question following on some of what was raised earlier. In addition to the competitive concerns about not wanting to reveal the fraud basis points and the volumes, another objection that typically is raised against collecting data like this in the United States is that it could have these adverse effects on consumers and may drive up their concern about fraud. You have been publishing these data in Australia and France for several years now. Have you seen any evidence that the publishing of these data has in fact created some negative concerns among consumers or has the reception been positive or nonexistent?

Mr. Stervinou: Yes, it does get a little bit of media attention, especially for CNP fraud on the Internet. But this is always an opportunity to underline safety behavior on the Internet for your consumers. I did not talk about that, but the way we publish and do the press conference around it is to also send reminders on how to properly transact online, such as to go to websites you know, to not leave your cards somewhere, those kind of basic things. Reinforcing the message that you have an instrument that is not perfect—it has security but it has fraud—helps. You, as a consumer, can do something about it. And the second thing you have to put in perspective is that the law in Europe now, with the Payment Services Directive since 2007, is very consumer oriented. This means that it is protective of the consumers. If you have an unauthorized transaction on your account, that being credit transfer, direct debit, card, whatever, you have 13 months to complain, to go back to your bank and to say basically, “I was not the one doing this, and you have to reimburse me.” And the bank has to reimburse you and then can investigate. This is very important. The directives or the regulations coming from the legislature in Europe have a tendency to defend the consumer heavily. That can be good or bad; I am not here to judge. But this is the way it works. That also gives some counterarguments to the fact that, OK, well it could raise fear, but in any case the consumers are protected by laws. So it is not the same.

Mr. Hamilton: Yes, I think that is reflected in Australia as well. In fact, if anything I would have said that now that we have a well-established process of issuing an annual, reasonably easy-to-read piece of paper and a six-monthly update, that has actually reduced the consumer fear and concern about fraud. Because having real data is a lot better than having fears, particularly when they are stoked by sensationalist television programs. Before we published fraud data, you would have “A Current Affair,” doing the latest exposé about some gang that is doing some card counterfeiting or something. Now, when they do that, they know they cannot get away without quoting the actual numbers and whether it is going up or down. So context provides some rationality to the debate and that is a really positive thing.

Mr. Sullivan: I just want to ask a unique question because I think Australia is the only country I have seen that collects and reports statistics on check fraud. I would be interested in Chris’ commenting on that. Why is it done, and is it as interesting as the types of discussions that we have had so far which is mostly on electronic payments?

Mr. Hamilton: You are probably the only person who reads that check fraud statistic. It is history. When we started doing it, it was a lot more important than it is now, to be honest. Checks are well and truly on the way out in Australia as they are in many, many countries around the world. So, any self-respecting fraudster is not going to go into check kiting, I am afraid. But that said, one of the reasons for getting going on fraud collection and presentation was a series of sort of nasty incidents partly in the check space. So it was a response to the environment.

Mr. Stervinou: Just one word on this because it actually is interesting. We also collect fraud on checks in France, but we do not publish, so not the same treatment as for cards. Interestingly enough, the absolute fraud amount for checks is very close to that for cards. The checks are still garnering a lot of transaction amounts. So, the person should follow up for checks in relative terms. This question gives me the opportunity to talk about the way to collect the data. With check fraud, we collect data directly from the banks, from the issuers. With card payment fraud, we collect data from the schemes and we also recently started to collect from the banks, not only to cross-check but also because it can help us understand as a public authority which banking network is better than the other, or which banking group is better than the other.

Mr. Dubbert: Gentlemen, thank you very much. An outstanding job. Alexandre, just tremendous progress. Chris, thank you for your views. I appreciate your insight.

Achieving a Resilient Cyber Ecosystem: A Way Ahead

Luncheon Keynote Address

Peter Fonash

I am not going to talk about payments. I am only going to talk about cybersecurity in general, and some of our efforts at the Department of Homeland Security (DHS).

First, I am going to talk about our responsibilities within DHS. I come from an organization within DHS called Cybersecurity and Communications. Within the federal government, there is a split role for cybersecurity. Each department on the dot-gov side, on the civil sector side, has a chief information officer (CIO) who is responsible for protecting in networks. The FBI and the Office of Management and Budget (OMB) also have roles. Our role, first of all, is to protect the dot-gov; in addition to the CIO's responsibility, we provide common services across the dot-gov domain. We also work with the intelligence community, law enforcement, as well as commercial partners, like the Financial Services Information Sharing and Analysis Center (FS-ISAC). We work closely with the FS-ISAC. In that role, we provide protection and we have a program called Einstein. You have probably seen that recently in the newspapers. Einstein provides perimeter protection; it is an intrusion prevention system. We have done something called "trusted Internet connections"—an initiative to reduce the number of connections to the Internet from agencies. In general, agencies are being forced down to two connections per agency. Einstein would be placed in line with that connection, and additional perimeter protection also would be in a "trusted Internet connection." That is the second thing we do.

The third thing we do, in terms of programs, is called Continuous Diagnostics and Mitigation, which gives you, at the enterprise level, a set of tools that, if you are familiar with the SANS Top 20, implements about 16 of the SANS Top 20. It does not address mobile security, but it gives you the ability to identify assets, to ascertain the vulnerabilities of those assets

and to do patch priorities. It reports to a dashboard up to OMB what is going on in that federal agency, and how protected they are.

We also run the National Cybersecurity and Communications Integration Center (NCCIC), which is composed of three pieces. The first, which is probably the most well-known, is the U.S. Computer Emergency Readiness Team (US-CERT). US-CERT is responsible first as a watch-and-warning function—watching what is going on in the Internet, and trying to give warnings if there are vulnerabilities detected or particular attacks detected. We also are going to start providing information in automated fashions, for example, reputation information. We are collecting information from many commercial sources on reputations, in other words, reputation of IP addresses, and we are going to be providing that shortly.

The second piece is the Industrial Control Systems Cyber Emergency Response Team (IC-CERT), and the third piece is the National Coordinating Center for Communications (NCC). I was at the NCC, and we were transferred from the Department of Defense (DoD) when DHS was created after 9/11. So, there is a legacy organization within NCC, up and operational, which is the communications ISAC; it also has responsibility for Emergency Support Function 2 under the National Response Framework (a guide to how the nation responds to disasters and emergencies). When there is a natural disaster like a hurricane or cyberdisaster, the different emergency support functions are activated, for example, transportation and health, and we respond and are responsible for managing the reconstruction of communications. Within that activity, some things we did were: during 9/11, we did the communications restoration for Wall Street and we had the responsibility for restoration of communications during Hurricane Katrina.

There also is the Office of Emergency Communications, and there are two priority service programs it runs. One is the Government Emergency Telecommunications Services (GETS), and some of you, I think, have GETS cards. That is for wire lines. And then there is WPS, Wireless Priority Service, which is for your cell phones. If you qualify for those programs, you can get priority communications over wireless and landline. The Federal Reserve has used those services in the past for restoration injection of currency into the marketplace.

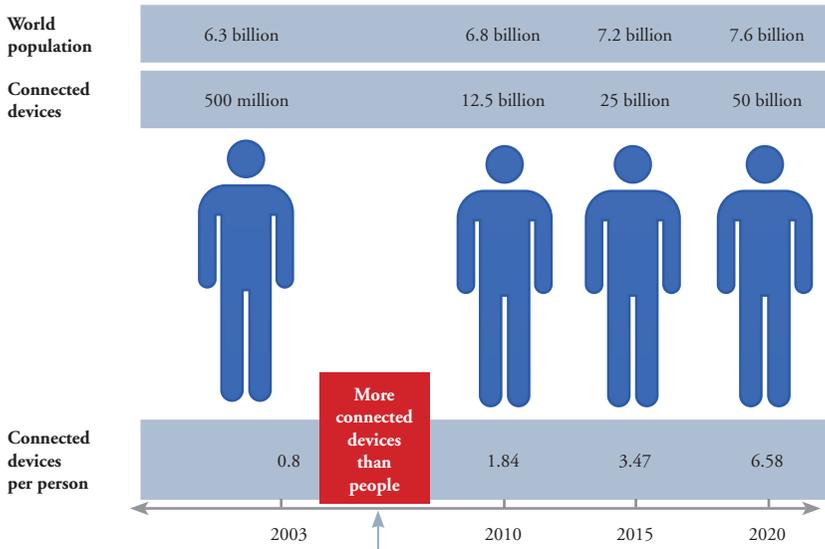
Now I am going to talk about what we call the cyber ecosystem. There are two reasons why I am going to talk about this. The first is that we are all in this cybersecurity problem together. Even though you think you are

secure, you have to make sure your supply chain is secure. You have to make sure your partners are secure because if you look at the Target intrusion, for example, it was not Target but instead one of its vendors that was actually intruded. And there are many, many cases in which the actual organization was not the one that was actually invaded, but it was through another mechanism. So, we are all in this together. It is an ecosystem, and we need to raise the overall security of the ecosystem. The second reason is that in addition to protecting dot-gov and critical infrastructures, we try to protect the general public and, in general, cybersecurity services in the United States. What we are trying to do with the initiative is to raise the efficiency and effectiveness of cybersecurity for the whole country.

I am going to try to go through where we are and why we should be concerned about doing things better. I hope everybody has heard about the Internet of Things (IoT). The point of this is that we have problems today in effectively providing security for controlled enterprises. Where we are going with the IoT, there are going to be all these devices—cars, refrigerators, home heating systems—that currently are under no one's security control. The number of devices is going to be in the billions, actually 50 billion (Figure 1). The figure shows we are really at a curve in terms of the use of the IoT: we have dramatically increased the use of it, and it is under nobody's security control. You are going to see auto manufacturers do things about IoT and address the safety of their cars. That is going to be a real problem as we get to auto-driving and things like that. You also actually can be attacked by your refrigerator some night when you go down for a snack. So just be aware. Attacks are continuously expanding. It seems like we get a new attack every week. Basically, the data breaches are increasing both in numbers and in scope.

In terms of how we are doing on cybersecurity, how we are protecting ourselves, there was a survey that said budgets in 43 percent of organizations are going to be flat from 2014 to 2015, so there is no additional money. Five percent are actually going to cut their cybersecurity budget. And 53 percent said they do not have enough people to do the job. We get into this efficiency issue.

It is interesting to note that based on the numbers from US-CERT, which are a couple years old, we had more than 160,000 reported incidents a year, and those are just the ones reported to us. There were far more incidents going on than the ones reported to us. Chart 1, taken from the

*Figure 1***The Internet of Things was ‘Born’ Between 2008-09**

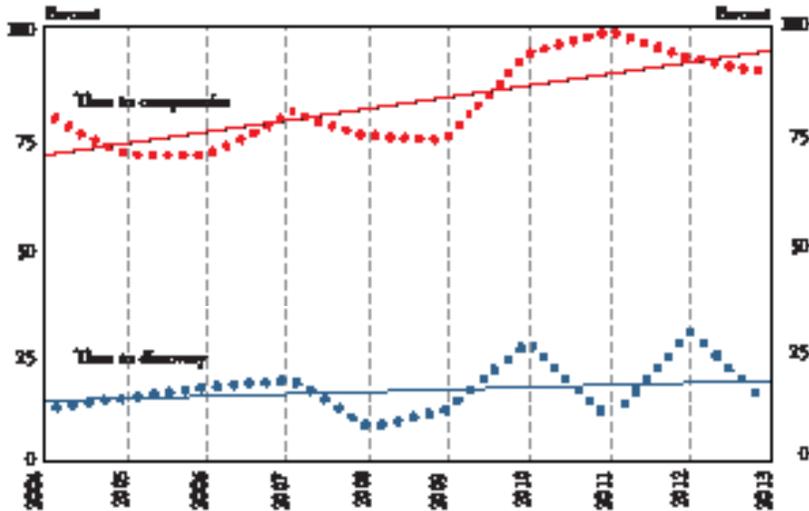
Source: Cisco IBSG, April 2011.

Verizon 2014 Data Breach Investigations Report, shows that in 2004, about 20 percent of the time we were able to detect intrusions in a day or less. And the bad guys were able to get in and attack about 70 percent of the time. There was a gap of 50 percent in how effective they were versus how effective we were. In 2014, that gap had grown. We were about 25 percent effective, and the invaders/intruders were about 90 percent effective. They have gotten much more effective and much more efficient than we have. They were better before, and they are much better now.

The challenges here, and why we need to get more effective, are the following. First, the security analysts that we have, every organization has, have incomplete knowledge of their individual organization as well as what is going on in the Internet in general. Second, adversaries are getting better and faster than we are. Our ability to detect and respond to intrusions is way too slow. There are some charts that show the average detection is 205 days, and the bad guys are getting in and out in a few days. That is a real problem. There is enormous growth in the scope of the potential cybersecurity intrusions because of the IoT. Third, trust among organizations is not sufficient to automatically share defensive courses of action; we do not share information. There are legal reasons why we do not, but there also

Chart 1

Percent of Breaches Where Time to Compromise (Red)/Time to Discovery (Blue) was Days or Less



Source: Verizon 2014 Data Breach Investigations Report.

are trust reasons—do I trust that you will protect that information, will you use it appropriately? People also are afraid they will give away some competitive advantage if they provide this information. Fourth, there is no resilient infrastructure that can support assured communications. What I mean by that is yes, we have those priority service programs, but right now we are moving from circuit-switch technology to next-generation technology, VoIP-type technology or IP-based technology, and we are not going to have the programs in place for about three or four years to provide those next-generation capabilities. So, the communications infrastructure is vulnerable to attack. I think 2017 is where we plan to start having operational capability. However, until then there is going to be a gap.

What I am going to propose is that we need to improve the effectiveness of cybersecurity. We need to make the analysts more productive. We need the ability to reduce the time to detect and respond from months to days or minutes. We also need to have much more innovation than we currently have in terms of the insertion of the innovation. There are a lot of innovations going on in the research community. I probably have six different companies come to see me every week—some of you probably have the same thing—telling me about new technology. But actually getting it out,

using it and putting it into an existing system is yet another challenge. We need to be able to better manage that process of innovation insertion. We do not manage our risks very well because many times we treat all data as equal, but all data are not equal. We need to move away from that model; we need to move to a risk framework.

How do we propose to do this? We feel there are solutions we can provide if we can get industry consensus on these things. For example, we need to get interoperability, automation, trust and information sharing. If we get those things, we will have much more effective and efficient cybersecurity than we have today.

What I mean by interoperability is that the tools we have today mostly are not integrated. Our analysts get data from different sources in different formats from different tools. We have to integrate those. Analysts are spending too much time manually changing the data or interpreting why these data look different than those data, even though the data are the same. That is why we have a manpower shortage; a lot of time is spent on rote efforts as opposed to analysis. If we can get to interoperability of tools, all with common semantics, understanding and syntax of data, then the tools can seamlessly provide data to the analyst. The analyst then will have a common understanding of what that information means as well as the tools.

Once you have interoperability, you can go much more to automation. We want to get to automated courses of action. For common events and common occurrences, we want to be able to detect something and then respond to something in an automated fashion. We do not want the analyst involved. We want analysts to be addressing the hard problems: we want to move the analysts away from being just involved in the rote activities to where they are actually being analysts and actually seeing unusual things. We also want to move to machine learning, so that the machines understand things better, see things and learn the analyst's intervention. After the intervention, a similar intervention is no longer needed because that would now be part of the machine learning of that environment. The machine learning will then allow the machines to take that automated course of action.

As for trust, go back to the idea that the analyst only has a partial understanding of what is going on in the rest of the Internet. We have to get to the point where we do much more information sharing, and to do that we need to have trust in partnerships so that people are willing to share

information. But we also have to resolve the technical issues of authentication mechanisms. Even if you have authentication mechanisms, if you do not have the trust, you cannot share information.

Once you have enabled interoperability, automation and trust, then you can really get into information sharing. That information sharing basically will be in the physical side of DHS. We want to use the motto “see something, say something” for cybersecurity. In other words, if you see something, we want you to report that to the rest of the community so they can take action on it and patch that vulnerability so that potentially they do not even get attacked.

Where are we today in interoperability and where do we need to go? There is something called orchestration, applications that turn tools into tool sets. The orchestrators basically manage—orchestrate—the activities of the suite of tools. They have to develop configuration files and things like that so as to get a set of tools to work together. You have to spend significant efforts in getting the orchestrators. Every time you bring in a new orchestrator, you have to redo that work. Where we want to get to in interoperability is that we have this common data model, common application programming interfaces (APIs), the tools just plug and play, and so the orchestration is automatic. We are going to talk about tools that do sensing, sense making, decision making, and an action. You want to have a set of tools that do these; you want to have a tool that senses an intrusion, then a tool that makes sense of that intrusion, then a tool that makes a decision on how to block it, and then tools that implement those decisions. That is where we want to go.

Where we are today in terms of future automation, again, we are at the orchestration level, but we want to get to automated response. This area is very controversial to many people who have concerns about unintended consequences. The National Academy of Sciences, and just about everybody else, has told me that is an issue. For example, if I detect something, I direct my firewall to do something and that firewall starts blocking normal corporate email. The unintended consequence is that normal business email is now being blocked. I did not think that was going to happen. It is an unintended consequence of an automated action. We need to get to the point where we have a much better understanding of what automation means and what are the consequences of that automation. We also have to have mechanisms to allow us to reverse automated actions, so we

can remove them very quickly once we see unintended consequences. We talk about getting the human on the loop as opposed to the human in the loop. Right now, the analyst is in the loop so that the human gets involved in making the decisions. We want to get to the point where the human is on the loop observing what is going on. That is where we want to move to.

In terms of trust, we have a lot of partnerships with the ISACs, and now there are going to be ISAOs, Information Sharing and Analysis Organizations. We are putting out a grant on ISAOs and we will be bringing out best practices through the ISAO Standards Organization so that information sharing can be done in an organized manner. The financial sector, by the way, I think, currently has probably the best information-sharing organization. The energy sector has a very good one as well, but you guys are clearly one of the leaders in that. We want to get to the point where we automatically trust those organizations. What I mean by automatically is I get information, and then I take that information and act upon that information. We are not there yet, but that is where we need to get to.

In terms of information, the right data will arrive in time to take that automated action. So see something, say something; you send that information out, and automated action is taken. That is where we want to get to. Everybody has a common understanding of what is going on.

So, then future communications. Right now we are transitioning from a circuit-switch technology to an IP-based technology. There will be some delay in capabilities for a while, but we need to have resilient communications because the assumption has always been that during a cyberattack you have communications and your security operation center is able to direct the response and recovery. What if they take out the security operation center, take out the communications? So, you need to address that too.

How are we going to do this? We, the government, are going to facilitate our ideas, but we want industry to lead. I am going to make the pitch that we are going to work with the IT industry on this, but we also want the customers of the IT industry—the banks and we are trying to get the healthcare industry as well—to say they want this because we believe we need to go there, but it is going to be market driven. There are reasons why the IT industry does not want to go this way, because right now they can sell proprietary solutions, and they make more money on proprietary solutions than open-based solutions. If we go to open-based solutions in

the very, very competitive IT industry, it is a market share issue. But we feel that the customers want this. I have talked to several banks and they seem to think this is a good idea in terms of where to go. We sent a request for information in January, and 58 companies gave us comments. We also had a roundtable with a much smaller group of industry. Banks were represented as well as the IT industry. It seems like the banks were in support of this. Even the IT industry was expressing interest. I think the IT industry is starting to see security as a service as opposed to providing a tool set. And I think what you are going to see is that as we go to security as a service, they are going to be much more open to having open systems, no pun intended.

So, we want to get to the point where we go from months to minutes and milliseconds in terms of our response capabilities. Part of the overall architecture, as we see it from the DHS perspective, is your example enterprise security system, which could be on the enterprise or in the cloud. You can virtualize the system into the cloud. You have sensing tools, sense-making tools, decision-making tools and acting tools, and they are managed by that management orchestration, and then there is a common database there too. The enterprise security system does boundary protection, infrastructure protection, host protection, endpoint protection. So, within that, there is a lot of information being shared in real time. It also provides information out to other partners, as well as to what we call the cyber weather map.

Our Deputy Under Secretary Phyllis Schneck talks about the cyber weather map. The idea is that we want to model ourselves like the National Oceanic and Atmospheric Administration (NOAA). NOAA collects a lot of information from a lot of different sensors across the country, and then has a model and runs forecasts. So, we are collecting information from the dot-gov domain, we also are getting information from the intel community and law enforcement and we are buying commercial information about what is going on in the Internet. We are starting to combine that information. We are not where we want to be, but we are collecting all this information, and then we will do analytics on that information. We are going to provide it to the enterprises, and we are also going to provide it visually. In the first part of what I call integrated adaptive cyberdefense, which, I should say, is a concept that we have been working on and partnering with the National Security Agency (NSA), there are three pieces; the enterprise piece, the weather map piece and what we call the AIS (Automated Information Sharing) piece, or the infrastructure that shares that information.

We are working this concept with NSA and we are demonstrating the concept in an integration lab at Johns Hopkins University's Applied Physics Lab. We are talking to different partners and doing pilots of this technology. We want to shift it to where we are actually getting faster than the attacker. We have done demonstrations and automations of this: in the laboratory/operational environment as part of the Applied Physics Lab we have been able to detect and self-defend attacks in less than a minute in the best case, and eight minutes in the worst case. In terms of sharing Structured Threat Information Expression (STIX) indicators, which are a threat sharing mechanism protocol, we have been able to share that information in less than two minutes in the best case, and nine in the worst case. We have constructed pseudo communities of interest, and we have been able to share that in less than a minute in the best case, and 45 minutes in the worst case just because of the architecture.

That is where we want to go. When we have looked at the effectiveness of this, and again this is in a laboratory environment with some operational capabilities, we have dramatically increased the productivity if you start multiplying those factors by that much.

General Discussion

Achieving a Resilient Cyber Ecosystem: A Way Ahead

Unidentified: My question is, as IPv4 goes out and IPv6 comes more into the norm, with the spoofing that goes on with IPv6, is that going to change how some of the tools work?

Mr. Fonash: I would think so. That is going to be an evolution. There are all kinds of problems. It is also getting more difficult to do security because everybody is doing tunnels and that is why you have to be very innovative. Innovation is critical here because it is always changing. We are always going to have to be rapidly changing security. If we just do the static model of how you do defense, it is not going to work because the threat actors are innovating quicker right now than we are. Part of the problem is that we do not have the standards. Right now we basically have a security cottage industry, which is being attacked by an automated adversary. We need to move to the Henry Ford model of the assembly line—as the products go down the assembly line, they are all put together and they all work. That is where we need to go with security, but right now the adversary is better equipped to be innovative than we are and that assembly line mentality and that standard set of data interfaces allow for innovation. We talked to a lot of the research organizations, like In-Q-Tel, for example: what we want to do when we come up with a standard is get In-Q-Tel, and other organizations like it, to ask that part of the funding it provides to companies actually be directed to the standard. Now, the other thing I forgot to mention was that the way we are going to get industry to lead this is by forming a CIPAC, a Critical Infrastructure Protection Advisory Committee. DHS has certain privileges under the law in terms of what it is allowed to create, how it partners with industry. The Federal Advisory Committee Act says that normally if government meets with industry, there have to be notes taken, the notes have to be very public and the meetings have to be open. Under CIPAC that is not true, and we can pick who we want as part of that

CIPAC organization. We are going to form a CIPAC to try to get these accommodative models and we got a very, very large IT security company to agree to be the lead chair. We are going to have industry lead this and we are going to ask the banks and healthcare to participate and get consensus on these control plane models, accommodative models and standard APIs. We hope to do standards, but we are not going to do API standards in the traditional manner. We are going to do standards in the sense of doing specifications and getting industry consensus. We are going to try to get to the 20 percent of the industry that controls 80 percent of the market and then the standard will become de facto. We develop the standard, test and prototype those concepts in our lab, show it works and then hopefully industry will adopt that. Eventually, when it is mature, we will make it a standard and go to the standards. We have done this with the STIX and TAXII (Trusted Automated Exchange of Indicator Information) protocols, which are the protocols for threat indicator information sharing. We developed a specification that right now is in the standards organization called OASIS (Organization for the Advancement of Structured Information Standards). So, we are making a standard, and there are 103 commercial companies involved in that standardization process. That is the idea of where we are trying to go and how we are going to have industry facilitate getting there. We are not going to do it; they are, but we are going to help them because CIPAC allows them to get together and come to a consensus.

Mr. Dubbert: So, Peter, could you discuss how you want the industry to lead here? The federal government is going to try to create the right incentives, perhaps the right foundational investment to ensure that the speed with which this can move along is acceptable. I think we can all agree we are behind the curve, we are probably getting increasingly behind the curve and you would probably agree with that. Talk about the financial and non-financial incentives you think will be the key factors that will motivate the industry to collaborate, like how we think about working together collectively as players in the payments system to collaborate and move that forward.

Mr. Fonash: First, we are going to have to form the CIPAC organization, but we are going to use our contractors, MITRE Corp. and Johns Hopkins Applied Physics Lab to do a lot of the leg work in the development of the specifications. Much of the financial cost of developing that will be borne by the government. But we also feel that what we want to do is try to influence future acquisitions. The idea is that once we get these specifications done, they will then become part of the contracting process for both DHS

and DoD. This CIPAC is not just DHS but also NSA. We are covering the whole federal marketplace with this. That is a big market driver, but not the significant gigantic market driver it used to be. If we get the banks as users and customers of that IT industry, along with healthcare, and if the IT industry sees that this is where they want to go, the incentive is either you go this way or you lose market share. But we will bear the large part of that cost of getting there. An example is SWIDs (Software IDs), which is a licensing mechanism—Microsoft and Adobe use it for identification of their software so they can verify if you have paid your license or not. But we are working with the General Services Administration to put that as part of the acquisition process. If you do an acquisition of enterprise licenses for software, you are going to have to use SWIDs. We are going to drive the federal marketplace to doing something like that.

Mr. Cunha: I know you are Homeland Security, and not world security, and not to complicate your job, but how does this connect with the rest of the world? It seems like you are driving all this as a domestic program, but most of these organizations are international and would not want to have a one-off for technology, products and services in the United States versus the rest of the world. Is there an international component to this?

Mr. Fonash: We do partner with other countries, and we also want to take this to an international standards organization so it will be an international standard. This is not going to be a government standard. Initially, it is going to be a U.S. specification, but if you look at the STIX example, that is an international standards organization and it is going to be an international standard. We already have the Europeans participating in the development of that standard, and we would see the same thing being done here. I also think that in today's world, the financial sector and healthcare sector, particularly the financial sector is a worldwide market. You are not just taking care of the U.S. market, you are taking care of the whole world market. You would want to make these tools be across your enterprise because otherwise you do not get the synergy you need because you cannot share information, you cannot get the automation unless you start doing this, and then you cannot get the innovation. I think innovation is really critical because in today's world it is hard to take a new technology and insert it into the large security environment because you have to ensure it all works together and that the information is understood. If you have all these data standards, you just plug it in there. The other example I give is like a motherboard. In the computer PC industry, they have standardized

motherboards, processors and the like. I can buy anyone's video card, anyone's motherboard, anyone's terminal, anyone's hard drive, anyone's SSD, and it all works because there is a set of common data standards, a common control plane and a common set of APIs. That is how they have driven the costs down dramatically, it is very effective. This is going to make analysts much more productive, enable us to respond much more effectively and allow innovation. That is the vision.

Mr. Hamilton: One of the problems we have been wrestling with, and I think you are wrestling with as well, is IP address does not describe a device. Have you thought about how we could have a more permanent IP device ID, and have you thought about using some of the commercial applications that are out there—Iovation, ThreatMetrix, 41st Parameter?

Mr. Fonash: So, that even gets into supply chain too, right? It is not just the device, but the history, where it came from and everything. Right now we are tracking this software through the SWIDs but we recognize that as a problem. We have not gotten to that yet. Hopefully, that would be one of the things we would address with this working group. When we get industry together, we are going to say, OK, what is the low hanging fruit, what are the things we can do easily, and then do those first.

Mr. Carlson: I am curious to know with the Internet of Things (IoT), given that chart in which you showed the growth in the IoT and the potential risks it imposes to multiple industries, if you had a magic wand in terms of requirements that you would like to see multiple industries adopt to mitigate some of the risks of the IoT, what would those be?

Mr. Fonash: I think you would want security built in as opposed to added on to the end. I also think you are going to have to go to security as a service. What I mean is, again I go back to the lowest common denominator—household partners, the power company and things like that—with which you have these power grids, smart grids and things like that. So, everyone is connected to everyone. Small and medium businesses and individuals, all they do today is buy antivirus; it does not work. We are talking about developing a technology at APL, and we are talking to a major ISP to see if we can convert that technology to security as a service. Small and medium businesses and people do not have the resources to run a security operations center nor the knowledge of how to do security, nor do they want to, nor could they afford it. What we want to do is get security much cheaper, and

then I can see, for example, the Internet service providers providing that as a service so all your devices would be covered. There also would be some type of network discovery tool that would discover your refrigerator was smart and your dishwasher was smart, which would then provide security over that. That is my personal view of where things need to go.

Mr. Dubbert: One last question: When should we invite you back to report on the implementation of all of these? Peter, thank you very much for being with us today.

Managing the Threats to Data Security



Moderator: Tracy Kitten

Ms. Kitten: It does not come as any surprise that the reason we are here today is all the data breaches that we have seen and the exposure of card data. I am excited about this panel today because we are going to review data security from many different perspectives. We are going to talk about some of the technologies and solutions in the marketplace—tokenization, point-to-point encryption—which is something Bob Carr is going to speak about—chip payments, behavioral analytics, transaction monitoring, biometric authentication to some degree, geolocation and even faster payments. During this panel though, we are not going to delve too deeply into the technologies themselves because the panel that follows is going to talk about devaluing data and the technologies being used. In this session, we want to walk you through a data breach scenario and look at where the industry has been, and where the industry is going. So looking at Heartland Payment Systems, for instance, in 2008 we all heard about that data breach. There were other breaches that were larger, but Heartland got all the publicity. Heartland was actually PCI compliant at the time of the breach, and it raised questions about data security standards. We have had a lot of data security standards come out since the mid-2000s, but as we see today, the way attacks are being waged were not foreseen when we developed some of these standards. In the past, and we still see these types of attacks today, social engineering was something we all worried about. I remember writing about ATM skimming attacks and we thought that was the worst thing we would ever see. But nowadays we are seeing malware attacks, network intrusions and data that are being compromised in the clear. So as transactions are being processed, the hackers are figuring out how to infiltrate that data.

We are going to talk about how all these things have progressed and what the industry needs to do in the future, and why we are not doing them now. First, Bob Carr is going to give us a presentation. He is with Heartland

Payment Systems, which experienced one of the first big data breaches in 2008. Bob is going to speak about what was happening then and what is happening now, and why we need to have end-to-end encryption to fix the problem. Then, Vernon Marshall with American Express is going to talk about some of the technologies and the solutions in the marketplace. 3D Secure came up in one of the earlier discussions and Vernon is going to shed some light there and tell us why the industry is not investing as much in 3D Secure as it should. Liz Garner from the Merchant Advisory Group will offer some perspective from the merchant side of the house about why making investments in technology is so challenging, especially for small businesses. When we look at EMV, tokenization, even PCI compliance, each is very expensive, and for entities that do not specialize in security, it is a daunting task. And then finally, we will close with Mark Carney. He is with the security intelligence firm FireMon. He is a Qualified Security Assessor (QSA) and has worked on a number of big data breaches. He can talk about gaps he has seen in compliance when it comes to PCI or some of the other data security standards we have, and some of the steps we should be taking but are not.

Mr. Carr: Tracy asked me to talk about what it was like to go through our breach, how we dealt with it, what has happened since then and what we are doing today. She mentioned that we were PCI compliant when we were breached, but that technically is not true. It is not possible to be PCI compliant and be breached. There is that elastic clause that says do not do anything that allows you to be breached; you are not compliant if you have done that.

It was actually 2009 that we learned about our breach. In December 2007, we had SQL injection into our corporate network, and we knew it, we found it, and we thought we had eradicated it. We had not eradicated it. It took six months, these people working day and night, to get over into our payments network platform, and seven years ago this month was when they got in. Albert Gonzalez got a lot of publicity. He is in jail now. He was the leader of the attack, but guess what? He was in jail in June 2008 when our breach started. We were being PCI compliant. However, as you know, PCI compliance is a point in time. And the QSA report that said we were PCI compliant failed to even look at one of our major data centers in Houston. For a long time afterward I said the QSA report was not worth the paper it was written on. How can you make somebody compliant if you do not

even look at their second largest data center and you are processing a couple billion transactions a year? We did not know that they missed Houston. But they did. We never thought PCI compliance proved we were secure; we never thought that for a second because the questions we were being asked by our QSA indicated he was not capable of determining whether we were or not. We were relying on ourselves.

So, we had the breach. Before that, we thought we had a pretty good record. We started with a valuation in 1997 of 10 cents a share, and in 2005 we went public at \$18. That was the story. You probably never heard of us before that. We did our IPO; we were 22 times oversubscribed, a higher rate than PayPal's. We shot up to \$27. Life was good. We actually got up to \$33, and then this. So, we decided—and this is a very controversial thing within our company—not to follow the advice of our attorneys and our crisis management company, who basically said: “Clam up, do not say anything. You might say something really bad that is going to get you in trouble. Just let us handle it.” And I said to the lawyer: “It sounds like you are trying to put lipstick on a dead body. We are not dead, and if we do that, we will ruin our company because we are a full disclosure company, we believe in being transparent with our customers, and especially our employees about what is going on.” There was absolutely no way we could follow that advice and survive. So, we called a hands-on meeting; I announced the breach. Within a half hour before the stock market opened the next day, we announced the breach. And the rest is sort of history.

What we did though is we learned about the Hannaford Brothers Co.'s breach in 2008. It turns out Hannaford's was the same breach we had; the same technology, same malware, same perpetrators. Three hundred other institutions were breached with the same attack vectors and the same malware. When I heard that, we were already trying to find an encryption technology that would encrypt the card number as it came into the system at the point of swipe. We could not find anything. We were talking to Semtech, but we were not able to work out a business relationship that made sense for our customers. In January 2009, we went to a company called Voltage; it was private at the time, now it is part of Hewlett Packard. We paid them \$10 million to invent the encryption for point-of-sale devices, and we could not get anyone in the United States or Ingencio to manufacture the devices. So we found a company in Taiwan that would build them to our specifications with our encryption technology, and we deployed those first

devices in July 2009. It took us six months to bring out this first device. We also had Voltage develop technology for our hardware security modules and our data center, and we came out with an end-to-end technology because we are a processor that has our own gateway, our own front end, our own back end, and so on. That was a major accomplishment in the industry, and we got a lot of credit. We also went to the Financial Services Information Sharing and Analysis Center (FS-ISAC), which has been mentioned multiple times today, with Peter Burns, who is the former head of the Payment Card Center at the Philadelphia Federal Reserve Bank. I asked Peter to help and he has been with us as a senior payment adviser since he retired from the Fed. And we worked with Bill Nelson from the FS-ISAC and we formed the Payments Processors Information Sharing Council, which I am proud to say is very robust right now. All the major processors are part of it, and we had our first meeting in June 2009. I am not quite sure what the exact saying is, but necessity was the mother of invention. Since that, we have come back fairly nicely.

Editor's note: Mr. Carr utilized a video as a backdrop to his remarks about Heartland's activities today. A transcript follows.

Video: During hunting season it is not safe to be in-scope. The same applies for merchants when it comes to payment card security. It is safest to be out-of-scope. A POS system that stores or transmits cardholder data is in-scope and more vulnerable to criminal activity. A system is also in-scope when card data is sent from a terminal to the POS. The POS system is directly within the data flow, a prime target for criminals looking to monetize stolen information. An out-of-scope system completely separates the POS from the card data. When out-of-scope, the POS sends transaction details to a Heartland secure certified device. The device securely communicates with the processor, then passes a response back to the POS. Since the POS never received sensitive cardholder data, it is out-of-scope, and less exposed to thieves. Stay safe and secure. Stay out-of-scope.

Mr. Carr: As the video suggests, keeping the point of sale out-of-scope is the answer to what we are doing now. We are rolling out out-of-scope in a significant way. We have continued to roll out our end-to-end encryption. About 100,000 merchants have our encrypting devices, and today we are exchanging unencrypting devices for \$180 and giving the merchant a standalone device that does end-to-end encryption, tokenization, as well as

putting their point of sale out-of-scope. Most of the breaches, the ones in payments, come from point-of-sale systems, and you have all these other things that allow the system to be breached.

Mr. Marshall: Just a little introduction to American Express. We are older than the Fed, and we issued our first charge card in March 1958. I have been with the company for 30 years and involved in fraud prevention for almost all of those 30 years. The company has invested a great deal in fraud prevention and customer service. Our goal is to provide the best possible customer service in everything we do, and as we have transformed as a company, that customer service has always been paramount.

I am going to talk about why I am optimistic about our industry's ability to control fraud over the next few years. First, EMV. I think this morning we may have underestimated the power of the smart card. When the U.K. implemented EMV chip, we saw a 60 percent reduction in counterfeit fraud. It was only 60 percent because some of the fraud could migrate to the United States. The United States is the last major country to implement EMV, and it will make a transformational difference. We believe chip and signature will give us about 80 percent of the benefit. We are preparing for PIN, but the industry is not moving to PIN at this point. Going to chip is the most important piece and it is a huge amount of work for issuers, merchants, acquirers and across the network. American Express will be mostly complete in our rollout by the end of 2015. We started rolling out cards in 2013 in anticipation of the October date. We are very bullish on the effect that the EMV chip card is going to have on counterfeit fraud. I guess that is one of the reasons why we have not seen those huge data breaches inside the U.K. For example, there is much less value in that data in other markets than in the United States. Swiped card data is hugely valuable in the United States because we do not have EMV chip cards.

The second big transformation, and I think this will be huge, is going to be machine learning. In May last year, American Express rolled out our machine learning system. We think it is the largest in the financial services world. It handles a trillion dollars' worth of transactions with an average response time of 1.2 milliseconds. We were a bit worried about whether our machine learning would have good availability. Availability since May has been 99.9998 percent—so almost six nines. Literally, any American Express card used anywhere in the world goes through our machine learning system.

So what is machine learning? It is a set of statistical tools that automatically learn from the data. Typically in the past, we spent maybe 18 months building a fraud detection role model, and we would have a large number of different segments. With machine learning, we ended up with a very large improvement in discrimination on something that I have been working on for 20 years, literally straight out of the box, with two or three days' worth of computer time. So we were stunned with the benefits of machine learning. It is amazing how quick it is to roll out a new version of the code. Next week, we will be rolling out our third version of machine learning, and we literally have two programs—one for the United States, one for all international markets—and next year, we will have just one program. It literally works globally, but it also finds any local fraud problems and just does a tremendous job at predicting fraud as it develops. We believe the industry will ultimately move to machine learning as well, and this will be beneficial across the industry. We think we will see the same on the acquirer side as merchants move to machine learning. The great thing is with predicting fraud, you have something that is very solid to predict; I have fraud transactions to predict. It is easier than predicting security issues across the country because we have a good problem to throw a trillion dollars of data against. If you can imagine, my job is looking at a trillion dollars' worth of transactions and coming up with the best possible variables that I can use in my machine learning algorithm. Every three or four months I can redo the fraud model to come up with the best possible prediction. So my job is probably the best in financial services. I have that ability. But I think other issuers and other networks will also move to machine learning quite rapidly.

The third real key benefit is what the customer can do to help us. With American Express, whenever we regard a transaction as suspicious, we send an email, SMS, push notification to somebody's smartphone and automatic voice response, and what we are finding is that customers are coming back usually within minutes. Almost 50 percent of the time, our customers come back telling us if this transaction is theirs or not within just one hour. So we are finding great strength coming to our models and coming to our system because we have the card members joining in our fight to prevent fraud. A huge change for us was announced last week where the Securities and Exchange Commission is going to simplify the rules for SMS or text messages in the United States. So now the United States will have the same benefit of text messages that we have seen in Europe and will make it much easier to reach card members and customers in the future. So we feel pretty

optimistic. I think the threats against the industry are probably greater than they ever have been, but we have never had tools as good as this. EMV to secure the card, machine learning to do the best possible fraud detection and multiple ways of reaching our customers.

Ms. Garner: For those of you who do not know about the Merchant Advisory Group, we are a trade association representing roughly 95 of the largest U.S. merchants, and our direct members are Treasury and finance professionals within those companies. We deal with issues related to payments, payment card security and mobile commerce, primarily, on behalf of our membership. I am on the panel to give you an overview and some insight into the merchant perspective on data security. I can tell you one thing: There is not a single merchant who wants to deal with a data breach. It is our customer and it is their security, and they have to feel safe shopping in our stores, either in a brick-and-mortar environment or online. Case in point. How many people in the audience can tell me how many Visa cards were compromised in the Target breach? Anyone? How many people can tell me how many MasterCards were compromised in the Target breach? How many people can tell me that Target was breached? That is my point. The reputational risk that card brands face is probably one-hundredth of what our merchant member companies are facing when we are talking about a data breach. We want to do everything we can to prevent a data breach at merchant companies. We just need better products, and we need a better playbook to get there.

I really liked the paper presented this morning by Tyler Moore and co-authored with Fumiko Hayashi and Rick Sullivan. I think it really delved into some of the big issues that we need to look at as we start thinking about how we move toward better fraud prevention in the United States. One of the facts out there is that we are grossly behind the rest of the world. We are still dealing with mag-strip cards, which we just saw were created in 1972. I would say that they are older than I am. That scares me a little.

Mr. Marshall: That scares me!

Ms. Garner: And we are still paying some of the highest rates and bearing a lot of the fraud in the United States. We do not get a payment guarantee in the merchant community on all payment card transactions. That is something all of our members are dealing with and we have to make this playbook better. So how do we do that? Open standards is one of the most

important things, and we heard about the incentive for open standards today. One reason I liked the paper, and I took a couple of notes on it, is it talks about how proprietary security technologies are used as a market tool versus coming into an open standards environment and going through an accredited process whereby all stakeholders have input to drive consensus on standards and have voting rights on those standards. When we do not have that, we have the will of the people who are driving that standards writing, or as we like to call it, specifications writing body, coming together and creating the rules of the road and the liability components to that too. One of the best things I saw on the slide presentation this morning dealt with, what is the small business dynamic of becoming PCI compliant? Well, the incentive is not really there because it is this Catch-22 that Bob Carr spoke about. You are not really compliant once you are not. And so that is a perceived limited return on investment for a lot of small businesses. We really need to look at how the rules of the road are being set.

There are a couple of direct quotes I pulled from the paper that are important as we look ahead to multipronged approaches to data security and whether the technologies are out there today. The first, “The proprietary nature of the EMV technology standard has provided global brands a competitive advantage over U.S. PIN debit networks.” That scares me a little. The second, “Due to the proprietary environment where the tokenization standards were developed, global card brands may have a competitive advantage at least initially in offering vault services compared with U.S. domestic card networks or processors.” Those are two really valid points. They suggest the need for opening standards, both from a U.S. competitive standpoint and from how we assign liability and bring the right incentives to get everybody into the fold to better protect the payment card ecosystem in the United States.

As we look at this multipronged approach, we have EMV, encryption and tokenization. None is really a silver bullet, but I think they are all technologies that put us in the right direction. There are some issues that we have to solve with EMV. We heard a lot about what happens to card-not-present rates. That is a huge concern for our members. Even those who run brick-and-mortar stores are tending to have more of a card-not-present environment, or a dot-com space right now. That environment is completely changing. For example, what does a transaction in a quick service restaurant look like in the next five years? Do I initiate the payment from my phone while I am in the drive-thru? How does that look under existing

card brand rules, and is it going to be treated as a card-not-present transaction? Is it going to have the costs associated with a card-not-present transaction? Is it going to have the liability terms associated with that? Those are all the things that merchants are thinking about right now.

Further, technologies we have been talking about, in particular EMV, tokenization and encryption, are not created equal across all proprietary specification groups. I think that is a huge concern for merchants deploying a mobile strategy because there are rules out there, at least the card brands in the legacy payments environment are saying if you accept our contact card, you should probably have to accept this contactless version as well. Now we are trying to take that one step further to say, well if you accept it in contactless, you should accept it on every device. Merchants are facing the dilemma of, if I turn on a certain type of technology, am I going to have to accept all the wallets that are accessed with that technology, or all products within a wallet that are accessed through that technology? That is a real challenge because not all back-end security technologies that go with those wallets and those products are created equal. That is one of the big things that keeps merchant payment executives up at night.

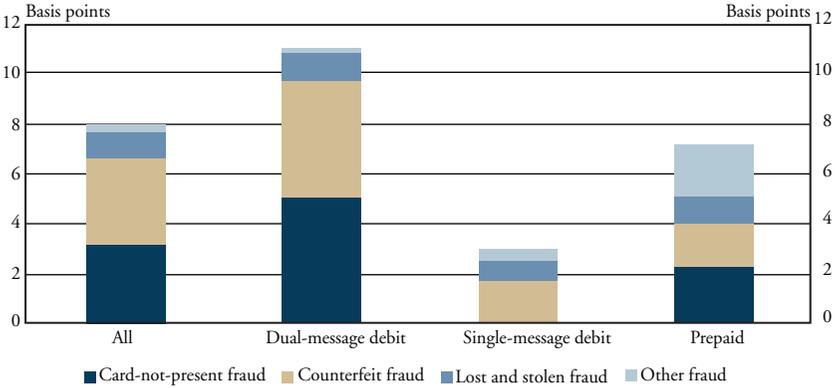
There is a lot of back and forth about why merchants support a PIN-enabled approach in the United States and there were a lot of questions about that this morning. I think Chart 1 says it all. Look at dual message fraud. It is 11 basis points. Single message, PIN debit, is 3. I could sum it up with just that.

Then, you look at Chart 2 and you can see how fraud is shared. This is Fed issuer data collected as part of the interchange survey released last September. This chart really says it all, why merchants and banks need to work together. Merchants are bearing 38 percent of debit-card fraud in the system today, issuers are bearing 60 percent and cardholders are bearing 2 percent. Where are the card brands here? That is a real problem when you are looking ahead and you are looking at who is empowered in the different standards organizations like EMVCo and PCI. Hopefully, I will get a chance to talk more about PIN when we go to Q&A. But I will pass it along for now.

Mr. Carney: I am going to lend a QSA perspective to some of the topics we have been talking about, particularly in three different areas—PCI data, post-data breaches and third-party vendor risk assessments and management.

Chart 1

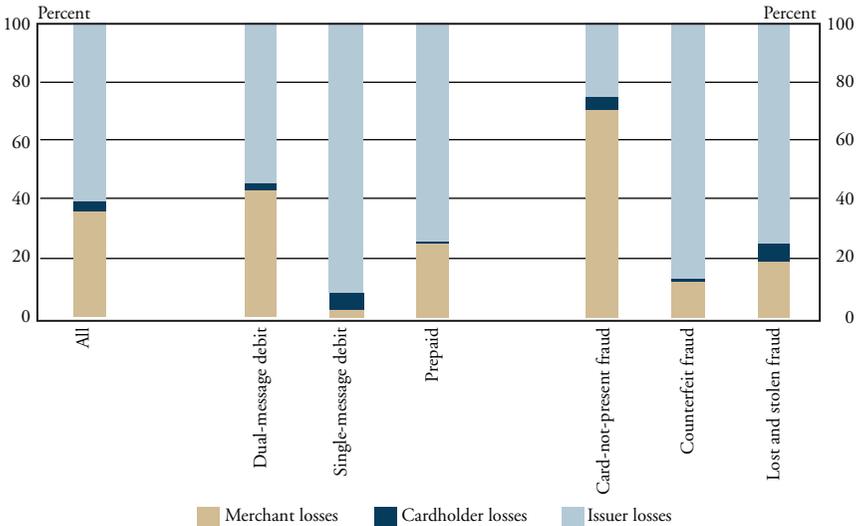
Fraud Losses as a Share of Transaction Value and by Transaction Category, 2013



Source: Federal Reserve Board of Governors. 2014. "2013 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions," September.

Chart 2

Fraud Losses by Transaction Category and Fraud Type, 2013



Source: Federal Reserve Board of Governors. 2014. "2013 Interchange Fee Revenue, Covered Issuer Costs, and Covered Issuer and Merchant Fraud Losses Related to Debit Card Transactions," September.

From a PCI perspective, we had this nice image of a stamp that says “PCI compliant.” Unfortunately, for a variety of reasons, we see a mentality from merchants that draws them to a kind of cost-efficient way to become PCI compliant. One reason is how PCI has been set up as a very prescriptive standard, which has a mentality of a checklist audit. One challenge from a QSA perspective is some QSAs have a very consultative, risk-based approach, but they are met with challenges around PCI standards, which are prescriptive. Also, the quality assurance process from the PCI Council is looked at as being black and white but there is so much gray; there are a thousand different scenarios within a particular report on compliance audit that need a more consultative, risk-based approach. Still, the natural tendency around PCI standards is to work up a checklist audit, which prevents the risk-based approach, which is unfortunate.

Another challenge is that virtualization, mobility, SDN (Software Defined Networking), and other emerging technologies have security implications. Any standards, and any standards bodies, have a natural challenge to keep up. The PCI standards body is doing a pretty good job, but it is still a challenge; they present guidelines, then some aspects of the guidelines eventually get into the standard, and then they have to allow for adoption. PCI 3.0 is an example. Some changes in 3.0 go into effect June 30, and they have provided time for the merchants to get up to speed on those changes.

A third challenge is that inadequate traditional technologies are not providing the protection they did in years past. Technology is fragmented. I came from a value-added reseller that sold 260 best-of-breed technologies and a wide variety of solutions. Multiply those types of solutions by four, five, 10 times; it is not only confusing, but also does not provide organizations a centralized platform for a holistic solution to protect themselves from breaches and to be prepared for them.

Probably one of the most concerning stories—I was at the Visa headquarters in Foster City, Calif., for some of the original training in PCI QSA. We were training with people who wrote the standard, and a lady raised her hand and said, “What is a firewall?” And man, did that just speak a lot to the confidence I had in the ability of some QSA representatives to do a quality assessment. I am proud to say to Bob Carr that the QSA firm at which I was formerly employed did not do your audit.

From a post-data breach perspective, we have talked about the shift toward card-not-present fraud. We are going to see a natural move to that

because of changes associated with EMV. We also are going to continue to see more malware, different variances and ransomware. A question will be how we approach ransomware when we encounter it. I think we are going to see focused-based attacks, by things like Dridex, which is malware that actually focuses on financial data and financial institutions. We also are going to see effects on the c-suite. We have seen that with Target, but even before Target, I was the executive sponsor for the Wyndham Worldwide Corp. breaches in 2008 and 2010, and interacted with their executive management along with the card brands, merchant acquirers, outside general counsel and others; there are many parties involved. They were under a lot of scrutiny as well, well before we saw the firing of executives at Target. Also, the civil suit associated with Wyndham was unique at the time.

The breaches we are seeing, and the Verizon breach report does a great job of reporting on this, seem much more sophisticated; like the attackers are ahead of us. We need to be very foundational and very logical in how we protect the data that is most important in our environment. We need to get back to the basics. A lot of the compromises are really from basic security 101 logic. We see a tendency of security organizations to buy a ton of technology. For instance, I built an information security program model, which is similar to the recently-released NIST Common Security Framework. It basically is a security program maturity model that allows a view into how an organization is managing its security program from a people, process and technology perspective, thus giving visibility into the types of security technologies bought and how those technologies are being managed (or mismanaged). We would go into these environments, and they would have 36 security technologies, and yet they would have five people to manage them.

Finally from a vendor risk perspective, there are a lot of fundamental flaws in the way organizations are assessing third-party vendor risk. The volume of vendor assessments is increasing, the questionnaires are not normalized, the approach is very tactical and each organization has a siloed program. While there are some organizations with a very complete vendor database, we need to create a stronger ecosystem of vendor-based security due diligence information and share that information across organizations. Companies like ThirdPartyTrust are trying to evolve third-party vendor risk assessments into an ecosystem that shares due diligence information in a central hub versus each organization managing siloed vendor risk management programs.

Ms. Kitten: Bob, you mentioned something about breach disclosure and how internally there was a lot of debate about whether you should talk about the breach and go into some of the details. Recently, there has been a lot of debate in the industry from a similar perspective. There has been a lot more legal discussion there. Target came out and was open about its breach, probably because it had to be in some regards. But when you look at other breached entities, such as Home Depot, there has been media coverage, but there has not been that much media coverage. How do you balance working with law enforcement, handling things internally, bringing in internal legal counsel to oversee a breach investigation versus working good PR and communicating with customers?

Mr. Carr: Well, it is different for a processor to be breached than for a merchant. So for merchants, it is a completely different situation, and I would not pretend to give them advice. Hopefully, no other processors will ever get breached. The processor that was breached prior to us was put out of business and lost their license, and we came this close to losing our license as well. The brands did the right thing by letting us have a shot at fixing the problem. Every company has its own culture and way of doing things, and whoever is making the decisions needs to be at peace that it is the best of a bunch of bad alternatives.

Ms. Kitten: Mark, you may be able to add something here from the QSA perspective. Does it hinder an investigation once you go public?

Mr. Carney: Going public and properly notifying law enforcement are the right things to do. I really like Bob's approach, the Heartland approach, versus say, Worldpay's approach, even though Worldpay got through its incident quite well. Openness and frankness bode the company culture and the executive approach.

Ms. Kitten: Vernon or Liz, do either of you have a comment?

Mr. Marshall: Not being a merchant, I cannot comment on that, but I agree that going public is helpful. Customers should be alerted to what has happened and when the breach occurred. It is most important to work with law enforcement, but entities need to go public. It is going to be found out anyway, so you should be public quickly.

Ms. Garner: I agree with Bob that we are talking apples and oranges with a processor breach and a merchant breach. The main difference is with a

merchant, you do not know if your card has been compromised if you are a cardholder who shopped there. According to the Verizon report, merchants did not even fall into the top three breached entities last year or the year before that, but they get a lot more coverage in the media because there is a lot more consumer uncertainty about it. Really, it is healthcare records, public records and financial institutions that rank above retail; at least they have the past two years, with a couple of other large-scale breaches. There is a different dynamic, and there are different dynamics between large retailers and small retailers. Having worked for the small business industry, for restaurants—90 percent small businesses, a heavily franchised industry—we had people who were contacted by networks that said, “There is some suspicious activity in your restaurant. We think you may have been breached.” But it is just that “we think you may have been breached.” How do you respond to that? And then you call your QSA and say, “How can you help me come sort this out?” And they say, “Well, we can come see whether or not you are on the hook for this amount.” And then the restaurateur has to say, “Well, but you are going to fix the plug, right?” The answer is usually “no.”

Ms. Kitten: And how you define a breach is a big part of it too. You can have a network intrusion and not necessarily define that as a breach. This is something we probably cannot delve into too deeply here, but there have been some recent discussions about once you start talking about a breach, whether it is internally, or once you start communicating with the media, or even law enforcement, if you do not bring in legal counsel to oversee that investigation, then all the communications are basically part of the investigation. If it is learned later that you hiccupped somewhere along the way, that can all be brought into the case against you. So it is an interesting discussion and one I am sure we will discuss more here as we get more questions.

Vernon, I would like to talk about the EMV liability shift, and because you have more of a global perspective, I think you could offer some insights here. Recently, there have been some discussions about how much fraud will actually be shifted back to U.S. merchants once this liability shift date takes effect in October. The U.S. market is not going to be completely EMV compliant by then. We all accept that. But how much fraud are European institutions absorbing right now from fraud that is coming from compromises here in the United States? How much fraud could be shifted from European banks back on to U.S. merchants after this October shift date?

Mr. Marshall: I think what is going to happen once we implement EMV is fraud in Europe will also come down significantly because the chip cards will have terminals here. I think it will be a minimal impact from European cards being used in the United States. So it will just be significantly less fraud.

Ms. Kitten: You do not think there will be a significant amount of fraud that will be coming?

Mr. Marshall: What we will see is within the United States itself, some of our counterfeit fraud will shift from merchants that have implemented EMV to the merchants that have not. So it is vitally important, especially for the small- to medium-size merchants, that they realize the October date is coming and implement EMV as quickly as possible. To try and help that, American Express donated \$10 million for a fund to provide \$100 reimbursement to smaller merchants implementing EMV. We tried to publicize that as much as we could. But it is very important for small merchants to move to EMV as quickly as they can.

Ms. Kitten: Liz, I know you probably have some thoughts about smaller merchants. Before we jump into that discussion about EMV wholly, I want to go back to something you mentioned during your presentation. You quoted Tyler Moore, and he made some good points this morning about the fact that when it comes to PCI compliance, it is somewhat misaligned, and that acquirers do have a role to play to help ensure the merchants they work with are maintaining PCI compliance. How do you think acquirers should be working with merchants, whether it is PCI compliance or EMV? Taking this step back and having a hands-off approach obviously is not working.

Ms. Garner: Well, acquirers are meant to be our biggest advocate. We do not have a direct relationship necessarily in every merchant case with the card network brands. We talked a lot about the private contractual relationships in Adam Levitin's presentation this morning. I think having a strong voice from our acquirer who understands merchant needs is one of the most important things for our members. As we look at the EMV rollout, we hope our acquirers will take an even louder voice to talk about some of the challenges we are facing. The reality of EMV in the United States is that we are lagging way behind the initial timelines. Nobody had really contemplated what it was going to mean to bring all the

domestic debit card networks into EMV, into smart cards in the United States. And that is an important part of preserving competition in debit card transactions in the United States and one that hopefully we would have dealt with otherwise, but are dealing with now because it is the law. We have seen a slow uptake in getting debit specifications out at market and that has put sort of a halt on the ability of merchants to certify with their processors to accept EMV. That is one of the big reasons we are behind. We work closely with our acquirers every day. They are our biggest partner and when we do get to EMV, it is going to be through a lot of work that they do to help us get there. In the meantime, we hope they will be an even stronger voice explaining to the card brands why we are not there. I will add one caveat. There are some question marks about who is on the hook for fees and fines when a data breach occurs, and we could look at the Schnucks Markets Inc. case where there was a lawsuit between Schnucks and First Data over \$500,000 and what point does the acquirer have the right to take that money out of the merchant's account for fees and fines due to the card brands. I think there needs to be more done to gather data on what is really happening there. You have a midsized merchant in Schnucks, but if you have a single unit small business owner, are they going to have the ability to challenge whether or not they are being treated as fairly as other merchants in the ecosystem?

Ms. Kitten: I think that is a great point. Mark, you were talking about PCI compliance. Do you think merchants of all sizes struggle with PCI compliance, just in different ways? Oftentimes we say small businesses struggle with PCI compliance, but I wonder if there are gaps in other markets too.

Mr. Carney: Large organizations have distinct challenges. For a large enterprise, I think it is scale and scope. Some of these enterprises are so vast in how they are interacting with cardholder data from a store process transmit perspective, along with the different types of payment systems leveraged. "Doing" the basics, like I mentioned earlier, going back to the basics is way easier said than done. Even when large organizations move quickly to remediate, and even put into place a newly designed architecture, it is tough to keep adversaries out of the network during this time period. These organizations are global in nature, they cannot even move fast enough to contain breaches if the attacker already has a certain level of access and that is why organizations can be compromised more than once. I think for smaller

merchants it is lack of knowledge. They really do not have the resources or the knowledge to respond and understand what is going on with PCI in general, even what PCI self-assessment questionnaire form to fill out. There is a lot of need for education with smaller merchants. There obviously is some great work going on with education for the smaller merchants today by the PCI Council.

Ms. Kitten: I am going to ask you this, Mark. I do not want you to speak specifically about any particular breach, but Sally Beauty Supply just comes to mind because it was breached twice. There were a lot of questions in the industry about whether Sally failed to eradicate the malware the first time around. Do you think a lot of these attacks that we have seen over the last 36 months have involved intrusions that actually took place a lot longer ago and we are just now discovering them?

Mr. Carney: Data definitely point to that; they suggest it takes 200 days before a breach is detected and typically, a common point of purchase is found by somebody outside the breached company. It is pretty consistent that more often than not, organizations do not have the required prevention, detection or even response maturity to be ready for a breach. Some are better than others, but it is more of a general statement.

Ms. Kitten: You made a good point earlier too, the fact that malware keeps evolving. So it is doing a better job of getting around fraud detection. Bob, I would like to come back to you, and if this is not a fair question we can hand it off to someone else. But we talked a lot about the migration to EMV and chip and signature as taking place here. Vernon seems to think that is a step in the right direction. Eventually, we will implement PIN. How strongly do you feel that we need to have chip and PIN?

Mr. Carr: I feel very strongly that we need to have chip and PIN. We are still exposed because a lot of devices are being made for EMV that send the PIN in the clear down to the processor, and that is just a recipe for disaster. Granted, that data cannot be used to manufacture counterfeit cards, but it can be used in CNP. So I understand it is very difficult for the issuers and the equipment manufacturers to switch over to chip and PIN, but that is where we need to be. I do not see why this lull of X number of years before going to chip and PIN is necessary. Chip and PIN would save one of the problems Liz was talking about for the merchants.

Ms. Kitten: You make a good point. I would like to talk about this migration of fraud. We have talked so much about upticks in card-not-present fraud, but quite frankly, we have been seeing upticks in CNP even with the existence of the mag-stripe. Do we really think there is going to be that much of an uptick? We looked at some examples today that show what took place in the U.K., Canada and France. But the market is much different than it was in the mid-2000s. Many transactions are conducted online. Could there be a channel we are missing where fraud might migrate to that we are not talking about?

Mr. Carr: Well, pity the merchant that is not going to EMV because as the number of EMV merchants increases—the large merchants are doing it much, much more quickly than the smaller ones—the smaller ones that do not do it are going to be vulnerable because the base of potential hacks is decreasing a lot.

Ms. Kitten: What do you think, Vernon?

Mr. Marshall: I am not entirely convinced that there is a link between EMV and card not present. What is going to happen is card not present is going to grow, and if I look at international markets, card not present grew when they implemented EMV, but card-not-present fraud in the United States also grew at a similar rate. The truth is we are living more of our lives online and we purchase more things online and there are more opportunities to steal data online and commit fraud online. So card-not-present fraud is going to increase, and not necessarily because of the EMV.

Ms. Kitten: Do you think there are channels we should be paying attention to that we are not?

Mr. Marshall: Across the industry, there will eventually be some concerns around identity theft. It probably makes as much sense for a criminal to migrate to an identity theft as card not present, so literally a calling card issue is in asking for cards to be replaced, and I think that might become endemic in the industry.

Ms. Kitten: Liz, I am going to give you a chance, but I want to ask Vernon one more question. Liz made a good point about mobile payments and how they will be handled. How do you think American Express will view a mobile payment that takes place when you are in the drive-thru? Will that be a considered a card-not-present transaction or a card-present transaction?

Mr. Marshall: There would be no liability shift to the merchant in that situation because it would be a mobile transaction. So liability would be with us, as an issuer, and not with the merchant.

Ms. Kitten: So it would be just like a card-present transaction?

Mr. Marshall: Yes, exactly.

Ms. Kitten: Liz, I think you wanted to add to that.

Ms. Garner: Yes, I was going to jump in on your question about where fraud is going to migrate. And I tend to agree a little bit on card not present. I do not think EMV necessarily is a hook, but it is lack of multifactor authentication on financial products. It is a travesty that we have a roadmap to EMV in the United States that varies so much from the international standards from an interoperability and competition standpoint. If we are looking to try to take fraud out of the U.S. payment system, as I mentioned in my remarks, we are one of the worst in the world when we look at global card fraud. One of the things that frustrates me the most is I get that it is a tough business decision for a bank to want to PIN-enable a product because there are concerns about whether the customer will be willing to come in and enter that PIN. Do you get to top of wallet if you put PINs on these products? And that is a business decision, and I get that is a challenging business decision to make. But it is not a security decision. If we are doing the right thing for security, we are doing two-factor authentication on all the financial products that we put out there. Unlike in countries such as France and the U.K., we have not had the technology built yet to accept online PINs or passwords necessarily. But we do have some commercially viable solutions in the United States whereby you can enter two-factor authentication online and that could help solve some of the problems and some of the migration of fraud into that channel. As I noted before, that is of utmost importance to the merchant. We are bearing 74 percent of card-not-present fraud right now on just the debit numbers alone. My members, who are very credit and e-com heavy, will tell me it is a lot higher than that, that it is almost close to 100 percent. So fixing CNP fraud is one of the top priorities for the Merchant Advisory Group and our members.

General Discussion

Managing the Threats to Data Security

Mr. Santhana: This question is for Vernon Marshall and Liz Garner. The future of fraud, as you all discussed, is in card not present and online account takeover. But if you look at the problem, we can do simple things that we are not doing today. On the merchant side, there is no standardization on capturing device data, IP data and proxy piercing. On the network side, they are unable to take device data and IP data and pass it to the issuers. So any thoughts on how we can improve those and capture all this data? You talked about machine learning. Machine learning can use that IP data and device data to do a wonderful job of looking at the devices that are related to a household, related at the account level and identify across different merchants as to what devices are using which card. So any thoughts on improving the data capture part?

Mr. Marshall: Ultimately 3D Secure is going to have to cover some form of device ID, and the problem is the large number of different device ID schemes. So it would be helpful if one of those becomes dominant, and it needs to pass IP address. I agree that is significantly helpful. 3D Secure needs to provide more data. It cannot just be reliance on a fixed password or a dynamic password because that too easily can be compromised in this environment.

Ms. Garner: You said in your question, standardization, no standardization. Standardization is a difficult word to use when we are talking about security because there are challenges that go with overstandardizing something. So back to my main point, it is important to lay the groundwork in an open competitive environment for how these technologies are going to work. We should not leave the development of specifications up to EMVCo and PCI when you have only a certain amount of input from different stakeholders at the table. No voting rights by merchants or really anybody outside of American Express at the table here. That is the first step. It is

a slow, painful process sometimes to go through an accredited standards-making process, but we have not changed the technology since 1972. We are on the verge of changing the technology to go into the digital environment. We have to get it right.

Mr. Horwedel: My question is this, in view of the fact that neither the merchants nor the merchant processors have any voting rights in any of the networks, in PCI, in EMVCo, and in view of the fact that the basic card product has remained unchanged since its inception 40-some plus years ago, why is it the merchants' and the processors' responsibility to protect the networks and the banks from their own product?

Mr. Marshall: I would get back to Tyler Moore's presentation this morning. For EMV to be implemented, the industry needed incentives for everybody to issue EMV cards and merchants to issue or build the EMV capabilities. Otherwise, EMV would not happen. So liability shift was the only way EMV was going to happen.

Mr. Carr: And we believe in encryption, point-to-point and end-to-end encryption, and I am not sure what more we can do than that.

Mr. Taylor: This is not for Liz because I know what her answer is going to be. I am going to make a statement, and I would like to get a comment on it. Increasingly, we talk about protecting the system and the ecosystem, and all the billions of dollars we have thrown at it, and you look at the card brands' own fraud numbers. We have not materially moved the needle which says the other guys are out-innovating us when it comes to protecting the system. Is it time for us to start forgetting about protecting the system, and start figuring out and focusing on doing clean transactions in dirty systems? And a second follow-on question, is EMV not really a deterrent and a distraction from doing that? Would we get better bang from our buck in trying to, to Bob Carr's point, take the value out of the transaction and the data out of these billions of endpoints that we cannot manage, instead of trying to lock down those endpoints because we cannot manage them?

Mr. Marshall: You need to solve the problem in both places, so both protecting the data in the first place, which we will be discussing this afternoon, but also protecting usage. EMV makes a huge difference in reducing the value of stripe cards. There is so much theft of stripe information at the moment because it is so valuable and it will be much less valuable after

October this year. So you have to do both. Probably though the quickest thing to do is to protect the usage.

Mr. Carr: I just come back to Governor Powell's comment. He said, "Preventive measures are not adequate." I completely agree. There is a lot of embezzlement in this world, and where does it come from? It comes from the trusted employees in companies. So we trust that our employees are going to all follow all the PCI procedures properly. But they are human beings. Sometimes they are careless, sometimes they are incompetent, sometimes there is a financial incentive for them to cause problems. All the preventive measures in the world are not going to prevent that problem with your employees. That is why I do not see why we do not spend a lot of energy, it does not cost that much, to do the encryption. It is a couple of dollars per device. And yes, you have to upgrade the devices, but it is not that expensive relative to going to EMV. But the industry has determined that encryption is not a significant part of the solution. I do not understand it. We have no skin in the game, by the way. We do not have any proprietary interest in anybody's encryption system. It is just, why are we not encrypting this stuff?

Ms. Walker: We have heard a lot about the private sector pieces on instant solutions, but I am curious. We are here at the Fed. What is the Fed's role in this, or what are you looking for from the Fed on this?

Mr. Marshall: One thing I would love to see happen in the United States is the same type of reporting that we have in France and the U.K. It would be very useful to be reporting fraud loss at a fairly granular level. It would be useful for us as a card issuer, useful for merchants and the networks. That is the most obvious thing the Fed could help with.

Ms. Kitten: I will jump in here too. There was discussion three years ago about whether the Fed would step in to oversee this migration to EMV, and it was made clear that the Fed did not want to play a hands-on role there. So it has to fall to the private sector.

Ms. Garner: The role the Fed is playing now is a good one in bringing stakeholders together to talk through a lot of the issues. That is a real positive. We are excited about the potential that the Secure Payments Task Force has. Publishing papers like the one they published this morning is also great. We do need to do more from a data collection

standpoint. That has been a theme throughout, and is something we would love to see too. From the merchant perspective, there is very little data available to us as well. That is one of the challenges when people look at, do I need to be going to EMV right away. Well, show us some more data that shows we need to get there yesterday instead of tomorrow.

But the bigger thing here is when we are talking about the policy dynamics, and this is one reason I liked how Adam Levitin laid it out, the public versus private trade-offs. In Washington, a lot of the regulators are looking at how do we respond to breaches? Do we pass a breach notification law? Do we share information after we are dealing with a breach, sometimes before? There is a lot more we can do in the fraud prevention space, and I am going to say something kind of out there that may be unpopular here at the Fed. But the Fed has a role to play here already. They have the regulatory authority to intercede in the marketplace. There is fraud prevention adjustment language in Reg II, also known as the Durbin Amendment, that allows the Federal Reserve to prescribe standards whereby issuers can receive an interchange fee/fraud prevention adjustment, and it asks them to take into account things like transaction mechanisms. Is it a PIN transaction, is it a signature transaction? You know the data that we put up on our slides about fraud losses, card-not-present fraud being borne 70 percent by merchants. Where is the trade-off here? We talked about if parties do not have the incentive to protect the data, do we get to where we need to be? And right now, issuers are not bearing a large portion of card-not-present fraud, and it is one of the fastest growing types of transactions in the United States. And one of the other components of that legislative language says the Fed should consider, what are the resources expended by all parties to deploy these technologies, and EMV case in point, some of the third-party groups out there said, you know, this is an \$8 billion project for merchants, and less than \$2 billion on the issuing side. I do not know if those are right, but if we start to think about, what are those trade-offs, there is a potential role for the Fed and we would love to see them get more involved under their current statutory authority in that space.

Mr. Carr: I just want to jump in and say the Fed is arguably the most respected institution in the ecosystem, and a lot of startups are innovating and trying to create solutions, some of the established players as well, and it would be great to have best practices recommended by an authoritative organization. That would be a lot better than what we have now. Look at what we have now. We have vested parties interested in promoting their own

solutions. I do not think it is working very well. And Eric (Grover), with all due respect, I do not think the free market system is at work here, before you ask.

Mr. Marshall: That said, it is worth remembering that the United States has the lowest fraud losses as an industry compared to other countries. We have a lower fraud loss than France, for example, as an industry. We have to have some sense of optimism that the free market system here is working at producing solutions. I am not saying we do not have challenges, and we were late implementing EMV. One of the reasons we were late is that our fraud control process has worked pretty well, even with ridiculously old magnetic stripe technology.

Mr. Horwedel: Is that because we have the best telecommunications in the world?

Mr. Marshall: Yes, that is definitely true. Certainly, over the last 20 years, we have benefited from being able to authorize 100 percent of transactions where it has taken much longer in other countries. That is true.

Mr. Santhana: We are banking a lot on EMV right now, but as Governor Powell said this morning, if you look at that fraud incident that happened in 2013 where \$40 million was compromised in 24 hours in 26 countries, cybercriminals actually went into the authorization system of the prepaid card issuer, and changed the limits. On the EMV side we are deploying, the dynamic card verification value (CVV) verification takes place at the exact same location, at the authorization system. Disabling that rule could allow counterfeit cards to transact because you are not checking whether it is an EMV card coming through. Do you foresee something like that? Are you fearful of that?

Mr. Marshall: I suppose it is possible. I think it is highly unlikely given the amount we have invested in cybersecurity, and that would be true of all of the major issuers.

Mr. Moore: I want to ask a question on a slightly different topic, going back to Vernon's points about machine learning and its value. There is a conversation about trying to get extra information to help make better decisions, and talking about getting device ID, IP address, I can see it evolving toward getting behavioral patterns of users and looking for deviations from their online behaviors. And the more we go down that road, the more likely we get into issues concerning privacy. I am wondering about your

thoughts on that, whether or not as we start collecting more data, passing it back to different players in the system, about the behavioral profiles of cardholders. Could that lead to an enhanced privacy risk by collecting and disseminating that data?

Mr. Marshall: Yes, that is a good point. The data has to be protected, only used for the purposes of fraud, not for any other purposes, and it has to be made secure, and for limited purpose. And the amount we collect should be limited entirely to what we need to control the transaction. I do think it is reasonable to receive an IP address and device ID for somebody that is making a transaction at a retailer. And retailers, of course, use that information to date to do their own fraud prevention. So it is reasonable to expect that the card issuers also, if they receive that data, could use that information to further protect the transaction. But I do agree there needs to be a ring fence around the use of that data.

Ms. Garner: I agree with that, and one of the things that scares me about EMVCo is they are trying to solve a problem we raised with the tokenization solution that they have out for comment right now. They have a payment account reference (PAR) number, but it seems like a lot of information could potentially be coupled with this PAR, where there is more insight into some of the transaction data, as well as other items we could couple with that data like a rewards program, than I am comfortable with as a merchant. The last thing any of my merchants wants is somebody to be able to come in and sell their competitor's purchasing data. So I agree, and it comes back to, for me at least, moving this more into an open standards environment to ensure we are not allowing people to gain market share by competing in that proprietary standards environment like the paper you guys put out says.

Mr. M. Williams: As a merchant, I agree with several of the comments that have been made about the use of PIN. It baffles me that we are going to all this effort in the industry and we are not taking the opportunity to fully implement chip and PIN. But what is more frustrating is the way it has been messaged, part of that being a comment I heard earlier, I am not sure who made it, "chip gets us halfway there," and then Vernon, you made the comment that this takes out 60 percent of counterfeit. I will politely and respectfully disagree with your comment that card not present is not linked. There are plenty of Fed studies that would indicate they actually are linked, and in some of those studies I have seen, at least two of four

countries that were studied actually saw an increase in fraud following the implementation. Now that is total fraud, but I get the sense that we are communicating this, especially to consumers and others that are not in this room, that this is a solution to the problem. I am curious, Vernon, for your response. What happens when there is a breach following the implementation of EMV, and those cards are able to be used online? How do you go back to consumers that you have currently told this is a solution, this will protect you, and then they are just as exposed? That is question one. How do you respond? And question two is, I am curious to hear from your perspective, what is American Express' justification for not putting PINs on cards? The only thing I have heard thus far is that it just is not what the industry is doing. But I assume, given that American Express has PIN cards in other countries, that there is some rational explanation for why it is not a good idea in the United States.

Mr. Marshall: I will start with the second question. At American Express, we have made all of our cards PIN-capable, and we are certifying merchants to process PIN. We will be ready to roll out PIN if the industry makes that move. What I want to avoid, and what American Express wants to avoid, is having to enter your PIN in one of every 20 merchants; that would be a disaster because you are going to forget your PIN. So the PIN rollout needs to be something that is orderly, and it needs to be when there is a significant base of merchants that are already accepting PIN, and we can roll this out at one time. I also think it needs to be an industry standard. Otherwise, it is going to be confusing to consumers to sometimes have PIN on some products and not on others. So we have made the decision to be ready for PIN and we have invested in PIN, but we are not yet ready to deploy it. But we expect it is likely that we will be implementing PIN at some point.

On the issue of compromising, if you think about it, for card-not-present fraud, you need a lot more information than just the 15-digit or 16-digit account number. All the compromising that leads to card-not-present fraud, you need the name, you need the address, you usually need the email address, you need the phone number. So for card-not-present fraud, the compromises for that are not point-of-sale malware, literally you have to go to the source of that data which is usually an online retailer to start with. So you do not see fraud, the Target situation, and any of those cards that were compromised at the point of sale, those details were not used to commit card-not-present fraud because it just does not have all the information criminals need to make the transaction take place.

Ms. Garner: I would have to respectfully disagree and I will just tell my own personal consumer story. I was traveling in Brazil last summer. I am a bit of a soccer fan. And I dipped my chip card at a card reader, and I could see when it prompted me for PIN, and I did not have a PIN, they were handing it over, “Hey, enter your PIN.” The tour operator looked at me like, “Oh, you do not have a PIN on this card?” I was like, “Oh great, this card is done.” It was done. Within 24 hours. They knew nothing about me other than the name on the card and the primary account number. Maybe they pulled the expiration date while I was not looking, but they did not have my email address or anything else, and they were making charges back to U.S.-based websites before I had left the city that I was in in Brazil.

Mr. Marshall: Without the details, OK.

Ms. Garner: Without all those other details.

Mr. Marshall: I guess it is possible. Most merchants would normally be checking the Automatic Address Verification (AAV), Address Verification Service (AVS) in the Visa/MasterCard world, they would be checking name and address for every transaction, and they also would be checking the three digits on the back of the card.

Ms. Garner: I am not going to throw anyone under the bus because one of them is one of my members. There were two very large sophisticated merchants where fraud was perpetrated online.

Mr. Marshall: You could advise them to at least do the minimum checking; that would be kind of helpful.

Ms. Garner: Well, we joke about this. But then people push back on me all the time and say, “Well, PIN is a static data element.” Well, Card Verification Value (CVV) is too, and we talk about a CVV capture as an extra authentication tool online. How good is that really? It is on the card. So somebody could have easily copied it off my card. Maybe they did it that way.

Mr. Marshall: It has gaps, but it is terrible to not check it. It makes fraud very easy to commit if you do not check it.

Ms. Garner: I promise I will not give you a hard time, so we will stop there.

Mr. Santhana: I have a question on network tokenization. I like network tokenization because it takes card numbers out of the ecosystem

completely. I do not understand why merchants need to have a card number to do a transaction. However, we have heard complaints from merchants saying they cannot track their loyalty programs. So what is it going to take to wean the merchant community away from card numbers as we move progressively toward network tokens?

Ms. Garner: I think there are two other reasons why merchants want access to the primary account number (PAN) and one is our own transactions fraud monitoring. We have not had very good e-commerce solutions in the past. So tokenization is not new by any means. There are several e-commerce merchants who have deployed some sort of a tokenization-like security technology for years. I was at an event with Amazon last fall where they said this is definitely not new to us. So transaction fraud monitoring is one area where we use that PAN and rely on that PAN to know the customer. And then customer exchanges and returns—that is one of the biggest challenges with the EMVCo token solution that is the back end for ApplePay. I cannot share an account with somebody necessarily and go back in with my Apple device and make a return or any type of exchange at the retailer because you cannot consolidate those accounts. There are some big challenges with how certain tokenization solutions are being deployed. That is not to say all tokenization solutions are created equal; I am just giving one use case.

Mr. Moore: I have a question for Mark Carney because he has not been loved very much in this panel on the Q&A. One thing I raised, and it came up here, is that there is huge variability in QSA quality, and the general evaluation quality for compliance inspections. I made this argument that it is due to information asymmetries, and maybe some adverse selection going on and the merchant is not selecting the best evaluators. I wonder what you or anyone else might think about how we might improve this process so the outside evaluations and certifications that take place are more valuable and actually say something about the security you are trying to evaluate?

Mr. Carney: I love that question, and I love having a question, so thank you. The initial Qualified Incident Response Assessor (QIRA) list was six firms. FishNet Security was the seventh. It was a very, very tightly controlled assessor list, basically for post-data breaches. I thought the quality of assessor sought by those that controlled this list was critical. They demanded a lot of qualifications, and the process to become QIRA certified took four to six months. Visa upheld a very, very high entry point

for a consulting firm to come in and represent Visa, MasterCard, etc., in these post-data breaches. To me, that is the best example of the PCI certifications that are out there. Certifications for Approved Scanning Vendors (ASV), Payment Application Data Security Standard (PA-DSS), the QSAs, and others are much different. When the PCI council took over the QIRA program, now called the Qualified Forensic Investigator (QFI), unfortunately what was observed was a watered-down skill set. At that time, the barrier for entry was lowered, and the quality of consultants representing QFI firms suffered. Not only that, the pricing pressure came along with new and more QFI firms making the list. Forensic investigators are not cheap to hire and require extensive training, so you have to have a bill rate that is correlated to the cost of a skilled person. Once that skill set gets watered down or there are more firms on the QFI list, then those are natural things that can hurt the quality of work for post-breach investigations provided to merchants/service providers.

Mr. Dubbert: All I can say is I am amazed at how much ground this panel covered in an hour and 15 minutes. That is a tribute to each of the panelists. Tracy, thank you so much for your coordination.

Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?

Moderator: Marianne Crowe

Ms. Crowe: Among the motivations for this conference are incessant cyberattacks and large-scale data breaches that expose millions of consumers' sensitive information and billions of dollars of fraudulent payment transactions. The previous session illuminated that even with the various security standards, protocols and procedures in place, the vulnerabilities to data security persist. And in response to merchants becoming more PCI compliant, hackers have moved on and now are focusing on exposing data in transit by inserting malware into merchant point-of-sale systems that then takes the clear text data as it moves and ships it to the hackers' databases instead. Then they are attacking the data instead of doing it at rest in the merchant databases and networks. Through such occurrences, we have come to understand that while a merchant may be declared PCI compliant at a point in time, as was said earlier, there are still unknown holes and missed patches and other gaps that can invalidate that. The migration to EMV chip in the United States is going to protect card data from being used to duplicate the physical card, but, as we know, it is not going to stop hackers from stealing EMV card data as it travels through merchant systems if it is not encrypted. Hackers can still expose this data and then sell it for use in making fraudulent card-not-present transactions, for example, in the growing e-commerce space, as was discussed in the earlier panel. During this panel, we are going to discuss technology alternatives to better secure and devalue data. I am very happy to have four really great experts in both the payment and security field on the panel this afternoon: Steve Schmalz, Radha Suvarna, Madhu Vasu and Branden Williams.

To begin our discussion, I want to frame the task by stating how payments data security has been viewed to this point. One ideology was to build a better wall to protect the data, and I think it can be argued that much of what we have been doing has been building these higher walls.

PCI compliance, for example, falls into this category. There has been a lot of success on this front, but as we know and as we have heard, it is not perfect and criminals keep figuring out ways to breach those walls and find new ways to get into the system. There is no one solution to the security problem. Instead, we need a multilevel approach to data security and fraud detection as a strong defense. And it appears that momentum for building such an approach is starting to happen, and it is relating to how we can devalue this data and make it useless, which is the topic of this session.

In applying the devalue-the-data model, card networks, issuers, processors and merchants are employing security technology so that cardholder data is stopped before reaching the point-of-sale systems and is rendered useless, even if it is exposed to fraudsters. This three-pronged holistic approach envisions EMV chip, tokenization and point-to-point encryption working together to protect payment data from the beginning of the payment transaction through to the end. With that as an overview, I am going to ask each panelist to take five minutes to share perspectives from their organizations and what they are doing or planning to do to devalue the data. We are going to start with Steve Schmalz.

Mr. Schmalz: I want to talk about the work that is being done at X9 F6 on a new tokenization standard. Rather than talk about that particular standard, I want to discuss what, to me, has been an evolving understanding of what is tokenization. I hear the word thrown about. I hear terms like, “Use tokenization to protect the network,” “Use tokenization to protect the data at rest,” etc. Token has become an overloaded term. It might be helpful if I talk about what the group has decided to use as a way of defining categorized tokenizations within a payment card system. Before I do that, I want to try some comic relief.

Are any of you fans of “Red Dwarf”? It is an older show out of the U.K. But it is a great show, and there was an episode ... I have to set this up. There is a cat, a robot, a hologram and a human on a spaceship, and they probably are the last living things, millions of years in the future. And they are wandering around and they go through this portal and they end up a million years in the past. And the cat turns to the robot and says, “Well, what just happened? What is it?” And the robot says, “Oh, it is a rip in time. It has allowed us to move across the spatial continuum.” And the cat goes, “Oh, thanks.” It turns to the hologram and says, “What is it?” He says, “It is like a black hole that allows us to move through space and time.” It turns to Lister, the human, and says, “What is it?” And Lister says, “It is

a magic door.” And the cat goes, “Oh, well why didn’t you say so in the first place?” I tend to think that sometimes when I hear the term “tokenization” thrown out, it is thrown out as a magic door. It sort of automatically protects everything. So I want to try to put things in context. The tokenization standard that X9 F6 is working on focuses on what you might have heard of as a security token, whereas the EMVCo framework talks about payment tokens. Well, those terms are sort of accurate, but they also create a bit of confusion. Let me give you some background on the “security tokens.”

You probably all know that PCI gives you relief of some of the auditing requirements if you use tokenization. Where the tokens live, the token is supposed to be worthless, so you do not have to actually focus any effort in seeing whether or not there is any potential loss of data there. The tokens are supposed to be worthless to an attacker. And the reason for that is the credit card number comes in, bounces through the payments system, and goes from merchant to acquirer, usually at the acquirer it gets turned into a token, and then when the information comes back, rather than having the credit card number stored in repositories, the token is stored in the repository. That token, sitting in that repository, has a lot less value than the credit card number, and arguably it may have less value than an encrypted credit card number because encryption usually involves some type of key management, and you have to make sure that the key management is not exposing keys, which brings the auditors back in. That more or less is the birth of tokenization as a security mechanism.

Now with EMVCo, a token is created before the payment transaction takes place, and when the payment transaction takes place the token is actually provided at the initial point of sale. It may not be provided in a point-of-sale device, but initially the token is given over instead of a credit card number. And then the token works its way up. At the top, at the issuer or the bank, it gets turned back into the credit card number and then some type of information comes back down to allow settlement after the fact. What is the difference? They both are tokens, but why do they use the term payment token in one case, and security token in the other? You can argue, well it is a payment token because it can be used just like a credit card. True, but it gets converted back to the PAN (primary account number) in the back end to finalize the settlement, and then you can argue that the security token is still part of the payment process. I think a much better way of looking at this is to use terms that the industry uses, and that we now use in our standard, and that is not to call it payment or security, but to call it a pre-authorization versus a post-authorization token. That

makes things pretty simple. Well, maybe not simple, but maybe it clarifies them. The term post-authorization simply means the token does not get created until after the PAN enters the system. The PAN is put in a point-of-sale device. As I described before, it bounces from merchant to acquirer, issuer/bank, etc. Somewhere along that process it gets turned into a token, and then when information comes back and you need to store what in the past would have been the PAN, you can store the token instead. So, the token is a pointer that allows you to get the PAN back when you need to. It sort of fills the void. It sits there and represents the PAN, but it happens post-authorization. The transaction gets authorized first before the token is created.

Pre-authorization simply means the token can be used to fire off the payment transaction. As such, it looks a lot like a credit card number, like a PAN, but is different in the sense that it can only be used in a limited scenario. It can only be used on certain mobile transactions or to maybe charge certain types of objects, etc. That pre-authorization token cannot be used at your local department store to buy something. You cannot swipe your payment token. You cannot swipe your pre-authorization token.

Calling it pre-authorization and post-authorization, I think, helps clarify what role the tokens are playing, and our standard focus is on post-authorization tokens. Now, that is the difference. There is a similarity in the sense that they do both provide security. Obviously, the post-authorization token is primarily a security mechanism. It is aimed at doing that. It gives very good security, but in a limited framework. It does not provide security for the whole payment process. It provides security after the initial authorization takes place. The pre-authorization token provides security, but it does it at a cost in the sense that the pre-authorization token can be used to charge things. So what happens in EMVCo's case, you do not just send the pre-authorization token, you send the pre-authorization token with some type of cryptogram. I am not going to go into the details, but there is a way to secure it, to make sure a hacker cannot use it on its own. You have to have access to multiple mechanisms to produce this package containing the token to actually charge something with that pre-authorization token. So in one case, you have purely a security function with post-authorization that is a little limited, limited to after-the-fact storage, etc. You have to put additional security mechanisms on the pre-authorization token, but it gives you more security across a wider swath of the payment authorization piece.

Hopefully that was not too confusing. You may be hoping that I had just described a magic door. But I think maybe it will help you keep things

in context. When you hear people say, “Why not just use tokenization,” that is a very vague term. The last thing I wanted to say involved what you might consider doing. I had a math professor who said a “Change of variables is good for the soul.” If you have ever taken a math course, you may understand. I would not worry about it, but the next time you hear somebody say tokenization, think: “Why not call it a funky crypto-object and tell me what you are actually doing with it. Tell me the protocol, tell me the system it is in; tell me how it is being used. Do not just throw out the word tokenization. Tell me what is going on.” And that is a far more educational experience than just using the magic door.

Mr. Suvarna: Just 30 seconds of background on what I do, to give context to my view. I head up emerging payments for the credit card business; basically driving this strategy of mobile payments and driving partnerships with networks and technology companies, industry players and wallet providers, bringing solutions to the consumers, and launching those solutions and driving usage and adoption. In that sense, my team’s responsibility is more on the business side. My comments and my views are probably more from a consumer and business perspective, and I might twist and tweak the technical definition of token.

From the perspectives of businesses, consumers, banks and the ecosystem, security clearly is important for a number of reasons and a couple of reasons most importantly. One is the adoption of mobile payments, or at least the evolution of mobile payments. For us to get consumers to adopt some of these new solutions, we have to get them comfortable and say, “Hey, use these, these are as secure if not more secure.” Because it is new, we need to step up and help consumers understand. Security becomes an important function there. The second is all the breaches. For those two reasons, we as an ecosystem and as a bank need to start thinking about security in a different light. The good thing is, as Marianne Crowe stated, there are now tools available—EMV, tokenization and point-to-point encryption—that we can start using to drive better value and enhance the security of the payment ecosystem. As Liz Garner mentioned earlier, there is no silver bullet. But put together, we can start to deliver a better, more secure solution for consumers. And without going into too much detail, I think the simplest way is EMV, securing the plastic and helping to reduce card-present transactions fraud; that may solve a set of problems. But it does not do enough to address the card-not-present transactions, for example. That is where tokenization comes into the picture and says, OK, how can you make the information less useful?

If you replace the actual card number with the token, suddenly we are saying that is more secure, and you might wonder why. You still are using the token to make the transaction. Why is it somehow more secure? I think the fundamental paradigm that I look at, and I start explaining to my executives, who obviously do not have time for understanding technology, is hey, here we have a 16-digit card number that is already powerful. If somebody can get access to that number, they can put it on a mag stripe and make transactions. They can go online and make transactions. They can do a bunch of different things. What if we could come up with another paradigm that basically says, you create a token and identify it for a particular wallet solution? As an example, Apple Pay. Or, you create another iteration of that same card number for a particular merchant, merchant XYZ. If that information is stored, customers can use it only to conduct transactions in that particular context because when that authorization comes in, say this token is coming in, it is assured for this particular wallet, but it is coming from this merchant or plastic, wait, something is wrong. Decline it. So, it is not making the chance for fraud zero, but it is reducing it; fundamentally, that is what tokenization does. Of course, you overlay EMV and point-to-point encryption and then it starts to become much more powerful. That is the very fundamental level of what tokenization is because it is a contextual number, changing the pattern from the all too powerful 16, 15, whatever digit, card number.

Now, from a banking perspective, getting and adopting some of these solutions and doing the security has value for the entire ecosystem because it reduces the disruption for consumers. It drives innovation and reduces fraud, which has a cost to the system. The last point I would make is that it is not going to happen automatically. We as an ecosystem and industry need to come together to drive standards around consistency of user experience. By putting consumers at the center—all of this technical talk is going to make sense for those of us who are students of this space—but at the end of the day for the consumer, it has to be simple. That is what we have to figure out, and that is what is going to drive ubiquity and adoption and actually solve the problem beyond the technology that it is today. I am looking forward to more discussion on that.

Ms. Vasu: I am privileged to be part of this panel. I am with the innovation and strategic partnerships at Visa. Since Radha and Steve covered a lot about tokenization and the standards, I am going to take a different twist and talk a little bit about my personal experience with disintermediation. We talked about new form factors in the payment landscape—evolving, changing the ubiquity of mobile devices.

An example that hit pretty close to home for me was I had the Starbucks application on my mobile device, and I was walking with a co-worker to the Starbucks in Foster City, Calif. I had the QR code, so basically what the Starbucks application does is it takes your payment credential, your 16-digit PAN, and it has what is known as a token, which is a QR code. But that token is basically just a mapping between the PAN in the back end. So my co-worker said, “You know, how secure is this?” And I said, “This is really secure.” This was about three years ago. So we did not get into tokenization, there were no standards or any of that at that point. So he said, “I am going to take a picture from my smartphone of your QR code and buy you coffee today.” And I said, “There is no way that is going to work.” But my worst fears came true when he was able to use his smartphone to take a picture of my QR code on my application and scan my QR code from his phone at a Starbucks counter ... and it worked. And my payment credential was being debited. That was a typical example where a payment credential was being passed through a different form factor, through different channels, and it can be compromised. The security of the payment credential was at risk.

Another example would be something like Google Wallet, where you have a MasterCard that is being front-ended. As a consumer, I think I have a Visa card in my Google Wallet and I think I am paying with a Visa card, and it is a card-present transaction because I go into a store and I use the Google Wallet. But what is happening is Google is basically front-ending my Visa card with a prepaid card. They submit the transaction to the issuer as a card-not-present transaction because they acquire the first transaction, which is actually a card-present transaction. I get an SMS on my device giving a different number from what I have in the Google Wallet, so there is consumer confusion. In the case of returns, I have no idea what the merchant actually saw. I think it is a card present, but the merchant sees a different credential. In case of disputes, the issuer sees a card-not-present transaction while I think it is a card-present transaction. Basically, as a result of all these form factors, there is disintermediation and confusion about chargeback rights. With respect to the tokenization standard, the EMVCo specification was put into place, and Visa’s part in that was we came up with what is known as a “token service.” We are working with the token requesters like Apple, Google, Samsung and other digital wallet providers, and there are certain key tenets that I want to drive home as part of this discussion.

When a token gets created, it gets provisioned on to a mobile digital wallet like Apple Pay. As part of the provisioning, the issuing banks are participating

in what is known as an ID&V process, the Identification and Verification process. In some of the earlier discussions, there were talks about why is it that we cannot use the device ID, why we cannot use geolocation, IP addresses of the device to make sure our risk decisioning is more secure? That is exactly what we are doing from an ID&V process. So, before the token gets provisioned, it basically is going through a risk assessment using these new nonstandard data. As a result, a determination is made whether a token needs to get provisioned or if a consumer needs to be subjected to additional authentication. They might have to receive a one-time passcode or call a call center and authenticate themselves again, or log into a mobile banking application and re-authenticate themselves. So that is the identification as far as provisioning.

The second component is transaction processing. During transaction processing, the token that gets transmitted during a purchase, when it hits our network there are certain domain restriction controls. Radha talked about domain restriction controls where the token is intended for just one particular channel, domain, or merchant. So those restrictions come in. That, combined with EMVCo cryptograms, makes a tokenized transaction more secure. It devalues the underlying data. Even if the token is compromised and used in a card-not-present transaction, it would not get authorized.

Mr. B. Williams: We have a lot of token talk right now. It has been interesting, but my experience at First Data, especially recently, where we have initiatives going on where we have a token of a token, or a token of a token of a token, feels like we are in the movie “Inception.” We are going down multiple levels of this thing. I think tokenization has turned into this year’s version of big data or cloud or virtualization, where people do not necessarily know what it means or know what it means to them. Frankly, I think a lot of people are afraid to ask the questions. So what I always tell people is do not leave a meeting until you really understand exactly what you are talking about, much to Steve’s point. Get down to the nitty-gritty details. Make that person explain it to you.

In the case of First Data, what we are talking about, is devaluing data right at the merchant; we think that probably is the right place to do it. We sort of have this end-to-end approach. We pull right from the swipe, and we devalue the card number there and replace it with a token on the way back down. At this point, the merchant and anybody in between, it could be a gateway or it could be somebody else, really cannot see that data. It is devalued in their perspective where it is just a stream of information that does not make sense

to them and what they get back is a replacement value that they can use for a number of different things, like chargeback, settlement, or clearing. Anything else like issuer loyalty and things of that nature.

Our goal is to really solve the bigger problem. I have done a lot of work in the PCI space. I think in the last five years, we have gotten to this point where the industry is marching along to the beat of the PCI drum, and nobody has stopped to ask why we are still doing this, does this really make sense, are we solving the problems that we need to be solving, aside from trying to reduce PCI scope by deploying technologies like this. With encryption keys, when we talk about protecting data in motion, there are a couple of ways it can be done. Asymmetric encryption is what we do for online types of transactions and symmetric encryption is where I have the same key to decrypt and encrypt. Symmetric encryption is typically a lot quicker; asymmetric is typically slower. But there are benefits to asymmetric encryption. In fact, we would not have online commerce without asymmetric encryption. So, they can be used to encrypt the same or different types of data, but the point is that it cannot be read.

Looking at tokenization technologies, the difference here is that encryption is what protects data as it is moving, tokenization is what is effectively going to protect it while it is sitting in the drive, sitting at rest. We strive to do everything possible with that payment transaction with the token after that token has been issued. From our perspective, what we call a token is a replacement value for the PAN. It is the same 16-digit, 15-digit number. In some cases, parts of it can be preserved so right at the terminal when the receipt prints it will say the last four digits so the consumer does not get confused in looking at the last four on the receipt. And we have had instances where merchants have had terminals go missing, been stolen, and this is before the settlement was batched for the day, and there was no card data inside of that terminal because it was all tokens. There was nothing that anybody really could do for a merchant.

Tokenization has another issue with single use or multiuse. In the case of a recurring charge, some of the tokens have to be able to be used, be presented for a reauthorization in the next month. So, there is another nuance in different types of tokens that you see.

Ms. Crowe: Since we are on the topic of tokenization, we will stick with that for a little bit. But I did want to go back to Branden for a second, and then the others can jump in. Since we are talking about multilevel security

and you mentioned encryption, how do Visa and Citi feel about the combination? Where do you see the value added, encrypting and tokenizing the PAN?

Mr. B. Williams: You can do one without the other, but I do not think anybody can get the value with one without the other. We talk about layered security. Or defense in-depth. Static defenses are not what we need; we need dynamic defenses, because static defenses can be compromised because you learn how the system works. And we did not solve for the math problem of elliptical curve. We just walked around the encryption key and got what we wanted. From our perspective, we can deploy one without the other; I do not know why you would. I mean, if you are looking to really solve the issue, which is to truly devalue the data as it moves not only through your system, but comes back and stays resident in your system, then you have to do both.

Mr. Suvarna: I think the simple answer is both of them will work together, and they are not alternatives. They are complementary solutions. Like I said, without understanding the depths of technology at the very simplest level, even the tokenization from merchant to acquirer, acquirer to token wallet, whatever it is, if it is starting with the network, the token wallet, the token is traveling, but from network to issuer in some parts of the transaction leg, the card information is still transmitted between points. So, at that point, if that needs to be secured as well, I am guessing point-to-point encryption is needed. So, at a basic level, I do not necessarily see them as competing alternatives, they are complementary solutions.

Ms. Crowe: One question that came up is if in fact it ends up being tokenized at the beginning, through the payment, all the way to the end, the pre-authorization and the post-authorization, and you go through all that process tokenized, does it down the road, maybe not right away but in the next few years, make the need for encryption go away?

Mr. Schmalz: No. First we are using the term encryption. I would like to use the term cryptographic mechanism because you can do a lot with cryptography other than just encrypt something. You can digitally sign something. So you can protect not only its confidentiality, the value of it, you can protect its integrity and you can do repudiation, and you can make sure people do not change it, and you can lock something in so they can only use a certain piece of that in a certain way. So when I say no, so you are talking about the EMVCo, what I call the pre-authorization token, that token is only secure because it does not get sent by itself. It gets sent with

cryptograms, which in essence are cryptographic mechanisms used to tie the token to the transaction and to make sure it cannot be used in any other context. I do not want to go into the details of the actual cryptographic mechanisms. So that is the first thing.

The second thing is at some point in the back end, it gets turned back into a PAN, and back there, I am hoping, it is not something I know a lot about, but I am hoping there is some cryptographic mechanism that is used to protect it. That may or may not be the case. So you have to think of systems here. Sort of back to what I was trying to get to before, to separate out tokenization from other cryptographic mechanisms and to isolate one and think that tokenization will give you all the security you need, that is a pipe dream. You have to combine other methodologies with it. In the case of post-authorization, the PAN travels in the clear without encryption. First Data, Heartland, they all do the same thing in the sense that they secure it when they get it between when it comes into the system and when it gets turned into a token. So you cannot separate the two. You have to look at it as a system; you have to look at the total protocol.

Ms. Vasu: I would like to add to what Steve just said. I do not think it is a one fits all solution for everybody. A hybrid solution based on the need that we have is very important. So a combination of encryption with tokenization and with also, for our merchant friends here, what we have is the payment account reference, the PAR, because they actually need the PAN back for loyalty programs, for fraud and risk, and this is something if we send in the clear today defeats the purpose of tokenization. So, we are working on the PAR, which basically gives the ability to tie the payment credential across multiple token requesters. It would be a combination of all of these technologies that would basically benefit, and I think isolating one from the other would not be very prudent.

Mr. Schmalz: The PAR is an interesting situation. The next time you hear anybody throw out the term tokenization as the end all/be all of security, without any differentiation, think about the PAR, because there is no need for PAR in the post-authorization token if you need the PAN back, you have access to detokenization services. In the post-authorization scenario, in fact, you probably do not want to give any detokenization functionality to anybody until the very top of the payment chain. But what does that mean? There are going to be multiple post-authorization tokens living in that system, and you as playing your part in the payment processing work flow, might not need to know what the PAN is, but whether it is the

same PAN being sent. In fact, there may be anti-money laundering requirements. So what are you going to do? Well, you have to have a mechanism like this. Here is an example where one size does not fit all. You need different security mechanisms, different pieces of data, to make them both work. That all being said, I know that Liz Garner mentioned that might be an issue from a security standpoint in ways that it might disclose information to others in the system. I am not trying to start a controversy. Actually, it would be fun if you guys had a discussion on that. But it is just something that you need to think about. It gets complicated. Even what looks like a simple solution gets complicated.

Mr. B. Williams: Why not take a real world example. For those of you who have Apple Pay, say you have been shopping at a merchant with your credit card for years. And now, the next time you go, you use your phone and you pay with Apple Pay. The merchant does not have the original PAN anymore. They have the EMV token that is your Apple Pay enrollment, so they cannot tie your new purchases to your old ones, just like Liz was talking about how you cannot pay with a credit card and refund with Apple Pay. So there is a situation right there where we have two different tokens or two different representations of the same individual. That is in one merchant. So the PAR is a different scenario where we can go across multiple merchants, we have anti-money laundering, loyalty, other things. We were just talking about at the coffee shop.

Ms. Crowe: Well, we can continue that with the Q&A afterward. But still talking about tokens and if tokens basically secure the payment credentials, we know the token service provider, whether it is one of the large issuers or the card networks for now, are storing the original PAN and doing the mapping when it is needed to be passed around the process. So what kinds of security, for someone who might not understand that, is in place to make sure the token vault itself is secure? Start with Radha and then Madhu.

Mr. Swarna: I would probably pass it on to Madhu. We do not have a token vault. We do not have this service.

Ms. Vasu: From a network perspective, it is sitting in a place behind our company's firewall, of course, and it is as protected as our authorization systems today so it is in a highly secure zone. The keys required for detokenization, applying the domain control restrictions and validating the cryptogram, currently exist within the network because it is a network token solution. So the token service provider is the only one who has the

ability to do this. There is a key exchange with the issuers in some scenarios, but pretty much the vault is the system of record.

Mr. Suvarna: Even though we do not have a solution, from an issuer perspective, the card credentials are issued by us, and they are already in our system. So tokenization does not increase the risk anyway, it is just the mapping. I am just clarifying. Tokenization, having a token work does not necessarily increase the risk. It is already there.

Ms. Crowe: So if I were Amazon or PayPal or some proprietary organization like PayPal, they have their own token vault for their back end or post-authorization tokens. Would they say the same thing, that is how they are protecting the security of their tokens in their vaults? Because they consider themselves token service providers for their own merchant customers.

Mr. Schmalz: Back in my QSA (Qualified Security Assessor) days, I helped a couple of different companies build something like that because there was nothing available. They built their own token solutions internally. I think what we are finding is that token solution still internally, it turns them into a bank or something that they are now having to protect, and a lot of retailers, frankly, do not take the same level of security that a bank or another financial institution would.

If I could give a quick plug to the F6 tokenization standard, those are exactly some of the issues that we address. We talk about how to secure what is called the tokenization service, which includes that vault. And we talk about how to securely talk to it, how to the secure communication, the authentication and authorization, the ability to ask for a token or detokenization services, etc. It is also important to point out that what the solution looks like depends on what the actual tokenization mechanism is, what the algorithm, for lack of a better term, is on the back end. Because there are multiple ways to do this. Initially the idea was that you had to randomly produce a token every time you saw a PAN, and that is how you produced this unique one-to-one matching. But the industry determined very quickly that it was just as secure to do something like 256-bit keyed AES (Advanced Encryption Standard) where you use format preserving encryption, but you only do it in one place, and you take that 256-bit key and you stick it in an HSM (hardware security module) that is some 140-2 Level 3. So the mechanism you use to protect it is different depending on the algorithm you used on the back end. But what is important, and this is very important to me, is that what makes the post-authorization tokenization “tokenization” as opposed to

encryption is the fact that it only happens in one or two spots, that there is a service where you have a lot of security protecting it, where you have to go to get tokens or to get PANs back for tokens. And so securing that is key to everything. If you do not do that, you do not have a secure system.

Ms. Crowe: I want to shift the conversation a bit, but stay on the tokenization theme; Apple Pay, Samsung Pay, I want to have secure elements in the phone that store the token rather than the PAN. And so we know that secure elements are considered, you always say tamper-resistant or tamper-proof, right? But then we have Google Wallet, which was mentioned earlier, or Android Pay, which I understand will use some type of tokenization, but they do not have a secure element; host card emulation and the cloud are involved. So can you explain how that is going to work?

Ms. Vasu: With Apple Pay it was a secure element implementation. And with the Android ecosystem, it is highly fragmented. In the case of Apple Pay, Apple owned the device, the operating system (OS) and they had full control over the real estate on the device. Whereas, with Android Pay, Google has more than 300 original equipment manufacturer partners. They have different partners who have control over the real estate, and to provision it on to the secure element is literally a struggle. So the shift in the industry was to move to a host card emulation where the token was provisioned in the cloud. But there are some security concerns as far as provisioning and keeping the credentials in the cloud. So even though it is a static token, the implementation model uses what is known as a limited use key. The limited use key is dynamic in nature, and it has certain parameters or thresholds like the number of transactions, the transaction amount, the usage, etc. So once these thresholds are reached, the token becomes invalid, until a new limited use key is sent back to the device. The token with the limited use key resides in the reloadable memory of the device, and that is how it gets protected, and that is how it is different from a secure element implementation.

Mr. Suvarna: I think that is an accurate description. Just looking at it from a slightly different angle, what we as an ecosystem will have to figure out is, one victory is obviously making it as secure as you possibly can; another is looking at how you can come up with a solution that is ubiquitous, drives consistency and gives you the value. I am not contradicting anything Madhu is saying. I am just adding. By going with the host card emulation, and it may not be as secure as secure element, but many more phones in the industry can become ready for tokenized solutions, and more consumers are walking around with more secure solutions than they

otherwise would have had. The net impact is that we are as an ecosystem more secure. I think we also need to collectively focus on how we are going to keep it simple for the consumer. We are just having to figure it out as space is evolving. We do not want to make consumers do too much work because they are not going to adopt. This could be a great technology, but without consumer adoption it is not going to be of much use. So we have to figure those things out. That is where standards come in, not just the technology standards, the specs and the likes, but also the decisions we are making to keep it simple for the consumers while ensuring every ecosystem's needs are being addressed whether it is merchants, networks, banks, issuers or wallet providers, to continue driving innovation. We just have to figure that out. I think the industry is making good progress. We just need to always have both lenses on, that innovation is not completely focused on making it as secure as possible, but you also have to have what is going to make it more ubiquitous and adoptable so we can have the right combination of the net effect.

Ms. Crowe: And that may mean a compromise between different stakeholders in terms of how and what standards get put out. So one question before we turn it over to the audience. We talked a lot today also about card-not-present and e-commerce transactions from a tokenization standpoint, but also the two other prongs of this devaluing the data in e-commerce. So for in-app and e-commerce, how do you see particularly tokenization playing a role? We talked about 3D Secure, but what about tokenization? Is that going to play a role?

Mr. B. Williams: It can play a role. It plays a role today. EMV tokens are what Apple Pay is, so it already plays a role. But I think that there is an opportunity for companies who have mobile apps to use tokens provided by their acquirer, store those tokens on the mobile device to be submitted for payment, as opposed to the actual card number. There are tons and tons of options in how it could be used and deployed. Whether that actually solves the problem or not I think is a really good question. We should look and see, does this actually solve the problem by adding all these tokens and adding all this additional stuff. I think it probably does, but we should probably look.

Ms. Crowe: Is Visa doing anything with it?

Ms. Vasu: We are using a TAVV, a Token Authentication Verification Value for in-app, e-comm transactions. However, I think liability will be the next question to come up. So we have not made any changes to the

liability because we are still in this mode where we are analyzing and assessing, because for us to effect a liability change, we need to make sure that there is issuer authentication at the time of the transaction. In the case of Verified by Visa, like 3D Secure, there is a password and a consumer types in a password to authenticate themselves that the issuer authenticates. But in the case of an in-app, that does not occur. So you do have a cryptogram with the associated token, but currently Visa's stance is we are evaluating and we have not made any changes to the liability.

Mr. Schmalz: The only comment I would make is tokenization does play a major role in the sense that you do not have to put the PAN on the card-not-present device. You can put a token instead, which I am just echoing what everybody said here. In addition, there is one last point I would like to make. These tokenization systems are systems, and whether it is card-not-present or any other payment system, you cannot forget that there are other things you can do to secure it other than just the controls of encryption, tokenization, authentication and access control. You can monitor, you can look for fraud. We have heard about that today. You have heard from the Department of Homeland Security, and everything that was said there was about monitoring transactions, put it in the language of payment, monitoring the transaction and looking for something funky happening. And that technology is just as important to deploy. So the name of this panel is if systems cannot be made secure, can the information be made worthless? Well, the answer to can the information be made worthless? Almost, but not quite. If the system cannot be made secure you better be trying to make it as secure as possible. So you need to hit both sides, and "try and make it as secure as possible" means multiple other security mechanisms need to be put in play.

Mr. Suvarna: I would only add to your question about should e-commerce and others be addressed through tokenization, and the answer is absolutely yes. I would go back to the same thing. Tokenization is a great technology, but the application effort, if it stays with mobile wallets and so forth where there is 0.01 percent of the transactions—I do not even know if it is that high—it is a great technology, solves the problem, but it is applied to 0.01 percent of the volume, what good is it? So obviously, we have to go and address and apply this cool technology and solution to where the volumes are, where we can actually get some benefits in the ecosystem. It is not a question of should we; we absolutely have to. The question is, how are we going to get there, and what sort of standards? For the right reasons, the ecosystem has started with the mobile wallets and so forth because that

is where it is easy to implement a solution now that we know how it works and there are kinks and we will figure it out. That is when we say OK, this is good, it seems to work. So now how can we take this and apply it somewhere else? That has to be the game plan.

General Discussion

Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?

Mr. Santhana: I have two questions. First one for the pre-op group, and the second one for the post-op group. For the pre-op group: Gemalto announced last October at the Money20/20 conference that they are about two to three years away in creating chip cards where the issuer can provision tokens at the point of sale. Have you had conversations with card issuers to see when that could be implemented, accelerated? I am talking about network tokens, NFC (near field communication) cards. In terms of your discussions with card issuers, do you see how that could be implemented?

Mr. Suvarna: Yes, in our case we are the card issuer. That definitely is an interesting idea. Honestly, from an issuer perspective, the way I look at it is there are digital wallets that are new, and then there is e-commerce that does a lot of volume, and then there are plastics where there is a heck of a lot more volume. So we have started with digital wallets. The next step is where do we go next, e-commerce or plastics? It is a matter of phasing in a new solution. Logically, it makes sense. Once we solve the e-commerce problem, then the question is, now that we have plugged those two holes, should we apply the same thing to plastics and does it make sense? And logically speaking, it seems to make sense. If there is a technology to figure out how you would put a token inside the chip of an EMV card that is different from what is embossed on the card, that sounds like the right thing to do, right? So I think it is a matter of evolution. There are other things to solve right now, and I think industry will eventually get there. It seems like the right thing to do eventually.

Mr. Santhana: But my question was will you be there in two years when Gemalto is ready?

Mr. Suvarna: Honestly, I would say in the space I am in, emerging payments and technology, two years is a long time. I cannot even predict what is going to happen in six months. So maybe; maybe sooner. Who knows?

Ms. Vasu: I agree with everything Radha said. And from a network perspective, if it is going to have the same format as a token on a mobile device, I do not see why we cannot support it and why the other ecosystem players cannot support it. It is just a question of will we start seeing those cards with the token on it that can be used in different form factors and also can be used to dip at a terminal.

Mr. B. Williams: Can I disagree? Panels are more fun when people disagree, right? So that form factor that you are talking about has existed in some form for a long time. I worked at Verisign prior to my time at EMC and we had one. So the question was, does this not solve a lot of problems? You have an algorithm right there, you can emboss a card number on it, they can hit a button, they can get a two-factor there, or we can just do tokens and issue tokens. You know, you have one vendor driving it in an ecosystem that may not be quite ready for it. We have to think about things like backwards compatibility. So, look at Apple Pay again. It is a backwards compatibility issue. The token is a 16-digit number, but it is a routable number. So while the issuer, Citi, gets a second set of BINs—they have their Apple Pay BINs and they have their regular BINs—we still have to think about that acceptance problem and how we get people using it. EMV is a perfect case study for how long it has taken us to get it and how in a lot of cases small merchants are almost being left behind.

Mr. Schmalz: If I could ask a question. So is the token being generated on the chip or is it being requested by the chip from some ...

Mr. Santhana: Requested by the chip at the point of sale.

Mr. Schmalz: So, you are just having a point-of-sale device make the request for tokenization or detokenization services directly and that is an infrastructure issue. Yes, that is fine. Then the tokens produced should be a token that is routable. So yes, there is nothing wrong with that. By the way, I would not call it a network token. It is a token.

Mr. Santhana: Maybe I should use “pre-op” versus “post-op.” So for the post-op question, the problem I see on the post-op side is now you are dependent on the merchant to provide tamper-resistant terminals and point-to-point encryption because the issue with tokenizing after the card information is captured by the device, at some point down the chain, is you are now dependent on the merchant implementing tamper-resistant terminals.

Mr. Schmalz: Yes, and you had the problem before, but you also had the additional problem of what do you do with the primary account numbers (PANs) when they come back. How do you store them securely? So you are

talking about an issue that is solved with chip and PIN cards, and you are talking about an issue that has been around for a while.

Mr. B. Williams: And by the way, we do that today. You do not qualify to get the tokenization encryption unless you have a modern terminal, which is going to meet all those requirements.

Mr. Moore: I would like to hear more of your thoughts on online and e-commerce applications. Forget mobile for now because it is 0.01 percent if we are lucky. And if I am entering my credit card number in my browser, I have this insecure computer that could have malware on it that could observe the card number, and then there is the potential storing of that card number at the merchants. There are lots of places where we have to share our card number in ways that could be compromised. Can you discuss what efforts, if any, are being considered in trying to devalue that card number and its use on computers and also on the merchant back-end networks?

Mr. Schmalz: That is an interesting question. What you are saying is if the computer is compromised, how do I prevent somebody from sniffing a credit card number, a PAN I just put on it? If you put the PAN on it, you cannot. Can you do something before you put the PAN on it? Yes, I guess you could produce a token that is not valuable before, but you would have to intervene. I just want to understand the question better. It seemed like a question where there was no good answer.

Mr. B. Williams: Unfortunately we cannot protect the consumer who has malware on their machine. They have to participate in their own rescue. They have to put their own tools on there to do their own things, and they do not want to do that because it is so much easier to just to hit “Buy Now” on Amazon; one-click buy. But then you talk about if the consumer is compromised and fraud is on that card. That smells to me like an issuer problem. The issuer is the one who probably would take the liability if there is no common point of purchase where they can sort of push it down the chain. You guys can correct me if I am wrong, but that is what it smells like to me, is that it is an issuer issue at that point. So then issuers today, they have fraud tools. If you bank with a major bank, you probably have had your card shut down at a very inconvenient time because they are “doing you a favor.” So, it happens. They are protecting their losses based on what they have. To me it is like two separate issues.

Ms. Vasu: Yes, there are a couple of things I would like to add. If it is malware on the computer itself, then there is nothing much we can do. We are in discussions with several companies in the browser business, and they

are actively looking at using tokenization, with the least impact to them. If they now have to enter a token instead of a PAN, they are going to have to redesign a lot of their Web pages and input different criteria, which is a huge effort. Some of the discussions in the industry right now are about keeping the same merchant website intact, but in the back end, we ensure that those websites are token-enabled. So there is a token that gets sent once the consumer enters this data. The concept of applying the token throughout the acceptance environment in the network to the issuer would still apply at that point. The question here is there are no standards, it is in the very early nascent stages, but we are having those discussions. That is just one part to solve for browser-based e-commerce.

Mr. Schmalz: There is one other point I think might be important to make. There is technology today where you can download JSP (JavaServer Pages) to a browser, which has the capability of basically taking a snapshot of the system and monitoring. We can notice when something changes, when it looks like your computer might be infected. So rather than say what do you do when a computer is infected with malware, to protect the data going in, you can say can you detect or have a chance of detecting endpoints that have malware on them and then alert the owner or refuse to accept online transactions from those computers. So there absolutely is a way; you might not want to support that as a company deploying these solutions, but I know from an authentication standpoint there is a way to download JSP, which basically takes a fingerprint of the device and can see things happening that might indicate if the device has been compromised.

Mr. B. Williams: I want to add to that because I think that is not a great solution for a couple of reasons. First, a merchant is never going to say, "No I am not going to accept this transaction." Merchants always accept the transaction unless someone tells them not to. Second, with that type of solution, you have created another antivirus blocker. I have to know what to look for to determine that something is wrong. If I have never seen it before, or seen behavior like that before, I might not actually know what to look for. The cleanest way that I have seen it done is very clunky for the end-user, but having disposable virtual machines that are downloaded on the machine one at a time. That is not going to solve for keyloggers, and does not solve for other things, but it does allow you to add some of that dynamic stuff where it is a one-use piece. But I like where you are going. I think there is some interesting stuff there. It is a bigger issue, bigger than payments, this problem of browser security and drive-by downloads and things.

Mr. Schmalz: Branden, that is a great point and it brings up that you need to balance your security mechanisms with the cost. It is always a

balancing act, and there are difficult decisions. It may be that you actually put up with a little bit of fraud because that is the cheapest way of keeping the business up and running and profitable.

Ms. Zhang: My question is related to software-based security. You mentioned that the HCE-based wallet is a software base. Compare that with a secure element-based wallet, Apple Pay-based, you go through some certification of the hardware. My question is when you implement these HCE-based, maybe this is for Visa and other network vendors, do you do any certification on how they manage the token and the keys in the user devices, make sure they implement it correctly? Especially you talk about the different platforms for Androids.

Ms. Vasu: Yes, we do the device certification whether it is an Apple device or an Android device. The device certification process will occur in both cases. The difference is the location of the token. One is in the secure element, while the other is in the cloud and in the device memory. Basically, to compensate for the lack of a secure element in the cloud, we have the limited-use key that I explained earlier. But as far as device certification is concerned, we certify in both cases.

Mr. J. Williams: One of the interesting things about trying to protect all these different systems is that you have to look at the business case. What has happened in the U.K. over the last three or four years is because of the movement of transactions to card not present, for reasons as we have heard earlier of the adoption of EMV, a lot of merchants wanted tokenization services. What has happened is the acquirer or the payment service provider sitting between the acquirer and the merchant has offered these services to the merchants to solve that particular problem. Of course, the business case for the merchant is it saves their PCI scope, minimizes their costs. But the business case for the acquirer is that it makes the merchants that much stickier as clients. So why have we not seen this as a business case so far? Is it just that we have not seen as much card-not-present fraud in the United States so far?

Mr. B. Williams: From our perspective, we do not create that sticky relationship. So in our contracts, they are allowed to convert back. We also have an instance now where you do not have to be connected to First Data processing to use this solution anymore. But I think that probably has hindered some of the adoption because one of the big problems is that merchants are afraid of technology lock-in. I think we are all afraid of that. We are all afraid at some level that we do not want to get stuck into some technology that ends up hurting us long term. So that may have hindered things for now.

Mr. Schmalz: I have seen white papers floated and proposals to have—I do not know if I am using the right term—but sort of a tokenization service proxy where you go to one spot and it would ping the various tokenization service providers. It would do translation. So if you had a First Data token, you could send it, it would talk to First Data on your behalf and get the PAN back and then maybe create another token for another acquirer it is using. I think an association for hotel owners might have come up with that proposal, which would solve that problem. Right now, the tokenization solutions seem to be acquirer specific; of course, the reason is because it is a good business case for them to do it. You need to find a business case for either cooperation or for some third party to take over that still allows the acquirers to play a part and add to the security.

Mr. Spittler: We are talking about tokenization. In what sense is tokenization important to competition? I have seen that we are more or less going to concentrating all the tokenization service to networks, instead to having usage of tokenization by all actors like acquirers, merchants. In which sense is competition increased when you use tokenization?

Ms. Vasu: I am just going to rephrase your question to make sure I got it right. So the question is we have a network tokenization solution, and who is the competition for that?

Mr. Spittler: My question is, is it competition? How do we increase competition with tokenization? Because I have the impression that it is more concentrating on networks instead of all actors.

Ms. Vasu: In the current set of implementations, we have the networks who are playing the token service provider role, but in the EMVCo specifications, we are not restricting it to just the networks. A large issuer, a merchant or processor could play that role. We do not have requirements today, and that is what the next version of the specification is working toward in terms of other entities becoming token service providers. Now, in the case of the network, it was convenient because we see both sides of the transaction from the merchant acquiring side, and the issuer side, and we have the numerics and the BIN management in place. But we are not restricting anybody from becoming a token service provider down the road.

Ms. Crowe: And I think that is our last question. Thank you.

Mr. Dubbert: Thank you, Marianne, for coordinating the panel, and all the panelists for being with us today. I will be sure not to throw the term “token” around too much; making sure I understand what that means.

Role of Industry Collaboration in Payments System Security

Moderator: Jonathan Williams

Mr. J. Williams: We are looking at the industry role in collaboration and how we can help protect our financial institutions and the payments systems from all the attackers that we know are out there. I would like to thank the Federal Reserve Bank of Kansas City for giving me such a wonderful panel of eminent experts in the field, each representing a number of different collaboration efforts, and they will be talking about that later. To avoid any doubt, they are representing their collaborations and not the organizations you might otherwise associate them with. They will be talking about how they work together.

I am going to set the scene for what is the role of collaboration. Some key questions we need to ask ourselves are those I am sure you got in third or fourth grade when you were trying to tell a story. They are the questions about who, what, when, how, and most importantly, why. And the reason why we are looking at collaboration is obvious. We cannot individually solve the problems, protect all our organizations, have all the intelligence in any one business. Therefore, we need to work together, share intelligence and develop common standards and common systems. We need to work for the societal good because all these things are trying to protect the whole system, not just our individual institutions, but a whole set of payments systems to protect all of our customers. That is the real driver. We need to act from a moral point of view to restrict the bad actors from gaining overall control of our payments systems. No one has all the cards, and we need to try and understand what key points we need to bring together as part of these collaboration initiatives, and to work together to be able to properly attack them.

There are different types of collaboration, and when we were discussing this in the run-up to the conference, there were a number of different ways we categorize collaboration. We can certainly categorize it in terms of who

are the actors that are collaborating. Is it purely the financial institutions? Is it IT vendors? Is it service providers? Who actually needs to work together to provide all of the expertise to combat the threats that we see?

There is a question of what we collaborate on. Is it purely on the systems security side, or do we need to understand how that might impact our business processes? Do we need to set standards within our business of how we deal with clients and how we deal with other actors in the system? And there is certainly a question of how we deal with external parties, including our consumer customers whose view of security tends to be fairly lackluster.

There is a question of when we engage. Are we setting standards so that we are protecting our businesses, or is it a post-event collaboration to try and ensure we remedy the fact as quickly as possible? And then there are many different ways we can actually engage. Certainly by looking at information sharing, but also by working out whether there are common means of procuring services. Maybe there is a common service we need to develop to protect our organizations. There are a number of different ways we can work together, and as I pass to the rest of my panel, they will be tackling these particular discussions for each of their different collaboration initiatives.

I would like to finish by giving you a perspective on some lessons we can learn from history. In the interest of transparency, I am not paid by any of the European tourist boards whose castles are mentioned here, and these are not potential scenes or sets for “Game of Thrones” either. However, I think there are a lot of lessons from the Middle Ages that we can learn from. We talked about ensuring our businesses are secure. Yesterday, we were talking about building the walls higher, and these are great examples of high walls. But there are all sorts of other protection we need to think about. Walls are one sort of protection. However, if you built a castle which only had walls and did not have any gates to get in or out, that would be pretty useless. Therefore, we need to think about the security of who we let into the castle, who we allow to do business, and how we identify them, who we let the drawbridge down for, who we close the portcullises on. The castle at Chignon in France (upper right, facing page) is a great example of the purpose of protection. That castle is geared to protect a particular physical feature, it is that particular mount. Therefore, one of the key things we need to think about when we are designing our security is to design it around the business, to make sure it fits the business need. It would be perfectly possible to

Cybersecurity Lessons from the Middle Ages



create a wonderful castle, maybe something like the Disney castle, which did not fit a business need and was not protective of all of the assets and all the data inside. Therefore, I think we need to be very focused on exactly what we are trying to protect.

Now I will hand the program across to Charles Bretz from the Financial Services Information Sharing and Analysis Center (FS-ISAC). Many organizations in this room are members of FS-ISAC, but I guess most of you are from the payments side and possibly do not have an IT relationship with them. So, Charles would like to introduce FS-ISAC.

Mr. Bretz: I will give a quick introduction of FS-ISAC. First, I want to thank many of you who are members; you are the reason we have this information sharing and have this organization. For you who are not familiar with FS-ISAC, we are a nonprofit formed in 1999 to protect the critical financial services sector from cyberattacks. We are owned by the financial services industry, so we are owned by the broker dealers, stock exchanges, card brands, payments processors that send transactions to the card brands, credit unions, banks and insurance companies. It is a financial services organization. We try to mitigate cybercrime from many different threat actors. After the 9/11 attack, our charter was expanded to protect against fiscal attack by sharing information. We process thousands of different threat indicators a month, sometimes thousands per day. I will get into how we are trying to adapt to that information flow, the speed of information. We have grown quite rapidly. We have 5,900 participating institutions. We have about 2,500 financial institutions bound by our operating rules, who are under nondisclosure, under contract to share their information under our operating rules.

A couple of years ago, our board of directors asked us to expand across the U.S. borders. So now we have members in Western Europe, Australia, Singapore and Japan. We are probably going to pick up some membership in South America very shortly. Again, it is in response to members like MasterCard, worldwide organizations that realized the threat is beyond the U.S. borders.

How do we share information? We have two security operations centers (SOC). Our original SOC is in suburban Washington, D.C. We also have a backup center under contract through IBM in Poland that allows us to expand the time zone coverage. Information goes both ways. It comes to the SOC and it flows out of the SOC. Government sources of information

are very important to us. We try to partner very closely with our government partners. And then there are private sources of information that we buy for our members using membership dues. Broad categories of member communications are information security, physical security, business continuity, fraud investigations and payment risk. What we find is probably 90 percent of the information comes from our members. The information from federal law enforcement and other sources is very important. But our members usually find out about the attacks first. That information comes in unfiltered. We try to coalesce that information and get it out to the membership. But the key to FS-ISAC is you as our members. Many of you work on the business side or on the payments side, and you are not an IT shop. When your organization joined FS-ISAC, it was probably from your IT chief information security officer, your CIO. That is the primary contact, but it has grown beyond that.

There are other ISACs, so there are other sectors. Nancy O'Malley is going to talk about some collaboration in the retail sector. Sandy Kennedy is going to talk about that too. For instance, FS-ISAC shares some information with other sectors. There is an aviation ISAC, oil and gas, there is a multistate ISAC that covers state to municipal government. Information could be shared between those sectors and FS-ISAC.

We have a number of information sharing and analysis tools. We keep secure repositories of documents. For instance, we have a playbook for denial of service attacks in its fourth edition. Those attacks sometimes come from state actors. Recently, some have been non-state criminal actors. Members have shared information on how to defend against denial of service attacks. That information is put in a secure portal, behind a lot of security. Many times members want information about how other members are reacting to particular threats, so we gather that with member surveys. Membership is so large and we have special interest groups, so we have different listservers for those groups. We do emergency calls when an event comes up. Sometimes we will have 900 or 1,000 members on a conference call to share the most recent information about a particular threat. We have semiannual meetings and they are very vibrant. We run three sessions a year on cyberattack against the payment processes. We run one for the United States and Canada, primarily against what we call the U.S. checking account. There is going to be one in Europe this year against current accounts. There also is one for the card processing group. The Federal Reserve has been very supportive, so we want to thank

the Fed for their support of those cyberexercises. Last year, 800 financial institutions in the United States and Canada participated in that exercise.

Now let me explain our traffic light protocol (TLP). When you share information under FS-ISAC operating rules, we color code the information. Red means restricted within a certain small group. That restriction is usually very short-lived. The small group works on the information and decides what is credible before pushing it out a bit more broadly. Yellow or amber means it can only be shared with FS-ISAC members. Green means it can be shared with the membership and partners, including our government partners. But when it goes to government sources, the Freedom of Information Act becomes applicable. White means it can be shared with everyone. We try to push out information at the lowest level possible to get the broadest distribution of information to protect the network.

We also have what we call circles of trust. Our membership is large with different groups that work on different issues. Groups will vet information, and if it is just for that group it might stay contained. But many times it goes out to a broader group. When that occurs, TLP is employed. For example, it might be TLP red within the cyberintel group or the threat intelligence council. And they are going to work on it and try to make it where the membership can understand, and then it might be pushed out very quickly with that analysis as amber to the 2,500 members who are under nondisclosure. And then if we can, we push it out green, which means it can be pushed out to all the support organizations that might be supporting your bank or your company.

I want to talk quickly about automation. One thing that has come up is the volume of information we push out at FS-ISAC is hard for our members to deal with. So that process is becoming automated. We have worked with the Department of Homeland Security (DHS) to develop a standard to speed up the process. The bad actors, the criminal actors and nation state actors can get into your organization quickly, and unfortunately, it takes a lot of time for those attacks to be discovered. There is a need to speed up the information, and the volume of information is so great our members asked us to find a way to automate it. Our members generously provided funding for a security automation solution. We are using a taxonomy developed by DHS, STIX and TAXII (Structured Threat Information Expression and Trusted Automated Exchange of Indicator Information), so we can have machine readable information that can be pushed out to your devices like

your firewalls, security management systems, your data integrity systems, and those types of things. That is what FS-ISAC does.

Mr. J. Williams: Thank you, Charles. Any questions from the audience on Charles' initial comments? I have one. It seems that over the last few years we have seen a change in the type of threat actors. We have seen it move from disorganized crime to transnational organized crime and state actors. How do you react to that?

Mr. Bretz: I will start with transnational organized crime. Those criminals are very sophisticated and their business can be very profitable. They are highly incented to attack our members. Because that business is profitable, they have a lot of resources. They can share resources and it just builds upon itself. That increases the need for collaboration. It is the same thing on the state side. A well-funded state actor has a lot of resources, and as you said in your opening comments, it is difficult for one financial institution to stand alone against the state actor. We need the members' information as well as our partnerships with government partners to help defend against that.

Mr. J. Williams: Thank you, Charles. Now Nancy O'Malley from the Payments Security Task Force is going to talk about how to secure cardholder present transactions.

Ms. O'Malley: Thank you so much. It is my pleasure to be here to represent some really interesting work. Yesterday, the presentation divided some of the work in the marketplace between public sector and private sector, and by way of characterizing this effort, it is purely private sector. But I am interested in finding out how we can take the work that has been done by this group and do more.

What is the Payments Security Task Force (PSTF)? There has been some information in the press; we would like to have more. PSTF is an initiative launched by MasterCard. Our CEO, Ajay Banga, was concerned about the progress toward migrating to EMV in the U.S. marketplace. As he encountered his counterparts and spoke with customers about their issues and concerns, he felt there was a need to foster a different level of collaboration at the most senior level in our marketplace in the payments security space. He launched this effort in February a year ago. The goal was to bring together c-suite executives from various organizations and to gain and secure their commitment to advancing solutions purely in the safety and security space. There was an initial meeting of the CEOs and they made a series

of commitments to be continuing participants. Those commitments were that they had to personally attend meetings and that they would expend company resources to advance initiatives the group collectively felt were the appropriate focus for the PSTF. It was an unusual and unprecedented activity. He reached out to his counterpart at Visa, who was glad to support this effort and join as an equal partner. That is how the PSTF was launched.

Let me talk about the structure of the task force and its focus. First was that we would have a senior executive steering committee, and if you can imagine bringing CEOs or c-suite executives from all the organizations, it was an interesting proposition—lots of strong opinions, lots of disagreement. But sharing and focusing on safety and security, and what we might do collectively to advance that was definitely a shared concern and a shared value. We also felt we needed a third-party manager to bring structure and appropriate balance because it probably was not going to work if MasterCard and Visa did that alone. We retained McKinsey to do that, and to foster that spirit of collaboration, to advance appropriate work streams and work efforts necessary to achieve our goals. Likewise, we appointed two individuals, one from MasterCard and one from Visa, my counterpart at Visa, Kim Lawrence and I. Together our role was to continue to advance the PSTF's day-to-day operations. Kim and I, together with McKinsey, are the project management office.

We said we need to put some structure and organization together. We asked what key things the PSTF needs to focus on that could allow us to make some real difference in the marketplace without getting bogged down in antitrust and other issues, which sometimes become obstacles to our collaboration in the industry. With the help of the steering committee, those were defined as tokenization and encryption, EMV (obviously that was the basis for the formation of this group in the first place), communications, and a group focused on the consumer experience. So, with each senior executive agreeing to provide resources, we had multiday workshops with technical individuals within their respective organizations who were in a position to make a difference and provide the input necessary to do the work.

In the tokenization/encryption space, we found, and I heard it yesterday in the presentations, there is a great deal of confusion in the marketplace about what tokenization is, how it is deployed, what the structure is today and what it needs to be in the future. And so that particular task force was

charged with developing a white paper to guide merchants, acquirers and issuers on how the technology should be used, and how they should make advances for their respective businesses and their respective markets. Of course, it cannot provide definitive answers to all use cases, but a series of use cases defined by these participants were designed to address how tokenization could be deployed in their specific markets and environments. Merchants, acquirers and issuers were engaged in these work streams.

EMV was where we started, and that was the history of the formation of this group, so a great deal of effort was then placed behind EMV. As that group formed, they learned a series of different things that needed to be done. First, there was a lot of confusion in the marketplace about where we were in our migration toward EMV. There were surveys that had been done, but none with regular cadence. They were all point of time. And so the participants in that particular work stream committed to contribute data. It is not 100 percent of the marketplace and it was never designed to be, but it provided a benchmark against which we could take these participants who represented 80 percent of the U.S. market from an issuing perspective, and measure their advancement of EMV from their perspective. Well, the measurement of EMV advancements and deployment from an issuer side does not really do us much good without also looking at the merchant perspective. Because there are so many merchants, it was impossible to effectively do a survey of 100 percent of the merchant community. Instead, it was decided the acquirers would work to provide data on what they had done to support the merchant community. Admittedly, it is very incomplete, but a good benchmark to measure, from a baseline perspective, the advancements of the deployment of terminals in particular.

Yet to come will be information on when we start to see chip-on-chip transactions. You can talk about the deployment of cards, the deployment of terminals, but it is really the enablement of terminals and then the traffic associated with chip-on-chip transactions that ultimately will start to give us a feel for how quickly we are advancing in the marketplace. Are we behind schedule, are we on schedule, are we accelerating? And although we can see that activity from a network standpoint, we really did not feel that just the network perspective alone would tell the full story. We are not there yet in the collection of all this data; we are not there yet in the publication of the data; but we are in process. Some might suggest we are a little late or behind the timeline, and that is probably a fair criticism. But the determination of this group was we have to start somewhere; we may

be behind the timeline but we need to start now and move forward. They are at a quarterly cadence to do just that.

Our communication work stream is the next interesting activity. The communication teams came in believing their goal was to talk to the industry about the PSTF's accomplishments. And to some extent that was the charge we gave them. However, we have quickly determined there are a host of communications issues around EMV and the market that needed to be tackled and the principal one was the consumer experience. We heard this loud and clear from the merchants who are participating. They had concerns about whether there would be a slowdown at the terminal, what their role would be, how much burden it would be to facilitate quick movement through the checkout line and other burdens to advance the work we were trying to do with EMV. What would be the merchant impact? That input was invaluable to the work that we wanted to do to overcome that particular issue. So, that interaction with senior officers from merchants who participated in the task force, and also a variety of different market segments, was really valuable to us.

The goal here was, and what our learnings were, that we needed to focus, to set aside our differences and find the pathway forward that could quickly allow us to make progress on advancing EMV. Another key element among these was the development of a value-added reseller qualification program. It is an interesting piece of work. It was designed to educate value-added resellers to play an important role in the marketplace to educate merchants on the value of EMV. More importantly, it discusses the implications of liability shift and what it could mean to them and their businesses if they do not get on board and work to advance the adoption of EMV in their businesses. That program was designed to streamline and eliminate obstacles the industry had created toward getting merchants into the program quickly.

Then finally, the last one is the launch of <http://gochipcard.com>. That is very recent. It is a consumer education effort done in conjunction with the EMV Migration Forum. I am sure many of you are participants and are aware of the work of the EMV Forum. All of the work of the PSTF was designed to support and tackle those issues that the EMV Forum had not been able to do, and to supplement their efforts and was done in coordination with them.

So finally, the PSTF's accomplishments; we have twice published quarterly issuer and acquirer EMV survey results, published and distributed

a payments security roadmap white paper, launched a U.S. EMV Value Added Reseller Qualification Program and launched the <http://gochipcard.com> education microsite. We believe these accomplishments demonstrate the commitment of our marketplace to work together, and how we can be effective when we determine we need to do so. It also demonstrates that we can find common ground to advance work that is critical to our marketplace. We built an integrated roadmap, which has provided great guidance in what to invest, when to invest and how to invest. We have overcome some real barriers and we are providing great data into the marketplace to inform decision-making by these key stakeholders and participants. And we are going to leverage this group to identify and anticipate issues in other areas that impact safety and security going forward.

Mr. J. Williams: Very interesting, the breadth of the collaboration and the number of different stakeholders you have involved. Any questions from the audience?

Mr. Santana: Nancy, you mentioned you have been running this Payments Security Task Force for over a year. What are some of the key challenges and lessons learned you could share with the Secure Payments Task Force as we embark on the same journey?

Ms. O'Malley: One key lesson from this is that at the outset, although this organization does not have a legal structure and it does not have a charter, it really is the commitment of the participants to build and foster collaboration. Our ability to do that, and the success that was derived from this work. We had folks with very different viewpoints, but we tackled some key initial things that allowed us to build trust between the participants and to demonstrate to each other how we can collaborate to move things forward. I think what is really exciting about the Secure Payments Task Force is this marriage of the public and private partnership, because there is only so much we can do in the private industry world to advance some of these really important initiatives. But when we marry that with the opportunity to work with the Fed and to tap into their resources and insight, to advance this and provide some structure, I think it really is an opportunity to take some of the work we have done and move it to the next level. So I would say, start small, find those things which we can tackle quickly together, agree on the spaces within which to collaborate, and what you are not going to talk about to ensure you continue to advance and do not get bogged down in some of the political issues that clearly surround some of these things. That would be my advice.

Mr. J. Williams: I would like to hand the presentation over to Sandy Kennedy from the Merchant Financial Services Cybersecurity Partnership. There is going to be more of a merchant perspective on these problems.

Ms. Kennedy: Good morning, everyone. There is a lot of attention paid to the conflict between retailers, card networks and banks. And while there remain significant disagreements and challenges, we really have been encouraged by the amount of collaborations over the last 18 months. Obviously, with the major breach that occurred with one of our members in December 2013, the Retail Industry Leaders Association (RILA) board of directors, which at the time was chaired by the CEO of Target, saw a necessity for us to come up with a plan to move forward in collaboration. The CEOs clearly saw the payments system as an ecosystem, and there was no way we could move forward in a collaborative way unless we included everyone in that ecosystem. So they gave us direction, and it was very clear. They said to collaborate where possible, only fight if we must.

The example I am going to talk about is how we acted on this direction immediately, and it was with the formation of the Merchant Financial Services Cybersecurity Partnership. This partnership started when I reached out to Tim Pawlenty at the Financial Services Roundtable and found we were likeminded on a lot of issues. We had the opportunity to agree on a number of things. There were going to be things we disagree about, but we were going to find those areas where there was agreement, and try and move forward collectively. So together, with an outstanding team that he had, and the RILA team, we pulled together 19 associations representing the financial services and retail industries from all different areas, sizes and formats. They were all at the table. And from that, we worked on five key areas. I think ultimately the dialogue exceeded most of our expectations, and in the end important relationships were forged. I think we were able to talk about areas in which we disagreed in a way that was productive. The challenge now is that the partnership has come to an end. It was never intended to be a permanent body, but it is important that collaboration continue, so we are going to look for ways to do that, and support and push that forward.

Based on our experience, there are five major areas where collaboration across the payments ecosystem is important. I would give high marks to two that we were involved in, a mixed score to one and probably a failing grade on two. The one I will give really high marks to is cyberthreat

information sharing. The ability to share with others in as close to real time as possible, information about attacks faced and how they can be defeated, is one of the most valuable tools in the retail cybersecurity toolbox. Through this partnership, we learned so much from the financial institutions that were involved, FS-ISAC and other organizations. With their help, knowledge and experiences we were able to put together a Retail Cyber Intelligence Sharing Center. This is a separate organization that will house the retail ISAC. It is almost a year old and I think recently there was a formal relationship formed with the FS-ISAC, which will be extremely beneficial to both sectors.

The area where I also would give us OK marks is the payments ecosystem in terms of long-term payments and our view on that. There is a tremendous opportunity right now in retail in terms of how we look at omni-channel mobility, the digital world. There are so many opportunities for how people are going to shop now and in the future. We had a really good dialogue across all the industries on what we need to plan for this next generation of threats and technologies. Tokenization was an important part of this discussion, and while tokenization is still a ways from being able to address card security in the near term, it has great potential in the long term. We hope the collaboration, development and eventually how it deploys continue.

The area where I give us mixed results was in legislation. Policymakers at all levels, state and federal, were looking at ways to reduce cyberattacks. The partnership really did help to inhibit, deter and distract lawmakers who were looking to do kneejerk reactions to some of the cybersecurity breaches that occurred in the retail industry. In working with the financial institutions, we jointly called on Congress to pass legislation on sharing cyberinformation, which provided liability protections in our sharing environments. The House of Representatives has passed this legislation, and we are awaiting action in the Senate. What we disagreed on was what data security legislation should look like. Banks want laws narrowly written for banks to be applied to the rest of the economy. Retailers have endorsed added standards based on more than a decade of enforcement by the Federal Trade Commission. We are still working on that and hoping we can come to an agreement.

An area where we have had challenges and straight out disagreements—I know Liz Garner talked about some of this yesterday—is standard setting.

Retailers have long been frustrated with the process with PCI. We have never had a seat at the table, never been asked for input, and so much of what PCI dictates affects how we operate as retailers. We think we have a meaningful perspective and input and would like to be part of that process as we move forward.

The area of greatest concern and disagreement is how to improve security on more than 1.2 billion cards in circulation. But before I get into the details of that disagreement, it is important to step back and look at the bigger picture. The threat we face from cybercriminals is enormous and evolving. They are tenacious and sophisticated. Given the scale of that threat, we must employ a variety of tactics to be successful. Further, it is our perspective that the important work we are doing to harden systems and share threat information is limited by one undeniable truth. Criminals know economics. They know how to look for information. They are tenacious at looking for information that passes through our point-of-sale terminals, and information that we capture. And it does not matter how thick or how high we build the walls, the bad guys are motivated to find a way over, under, or through. But while we are hardening these defenses, we need to focus intensely on devaluing the data, removing the incentive for cybercriminals to lodge these attacks in the first place. When Europe grappled with these issues a decade ago, the solution they employed was chip and PIN. As a result, we saw substantial reduction in fraud. Since then, nearly every other industrial country has followed Europe's lead, deploying chip and PIN. Not surprisingly, fraud, like water, flows to the path of least resistance. That is why fraud migrated to the United States. As we all know the payments ecosystem is in the process of migrating to EMV. Unfortunately, we are not moving to chip and PIN like the rest of the world. Instead, we are moving to chip and signature. With this migration, the United States will sadly retain its position of being the path of least resistance.

Retailers believe that we need, and have an obligation, to walk and chew gum at the same time when it comes to payments security. We must migrate to the best security technology on the 1.2 billion cards in circulation, and continue to work together to ensure our customers' security with new technologies and shopping opportunities.

Mr. J. Williams: As part of how we are dealing with innovative criminals, where can you innovate to try and protect your businesses against them? How can you drive and promote that?

Ms. Kennedy: The collaboration provides great insights into leading practices. We had been patiently selling things and really did not consider ourselves technology companies, which is what we are. We have become technology companies. And so we had to change our mindset and think differently. Again, through the working groups, there was a lot of sharing of leading practices, areas that our sites had never even thought about. From that standpoint, that allowed us to leap forward in our learning curve in this area.

Mr. J. Williams: Thank you. I would like to hand it over to Liz Votaw, who is going to talk about how we ensure exactly who we are allowing through the walls of our castle.

Ms. Votaw: Good morning. I am from Bank of America, where I lead and develop strategy for authentication across all the different channels in the consumer bank. But I am here today as a member of the board of directors for the Fast IDentity Online (FIDO) Alliance. I am not going to be able to answer questions about Bank of America, but I am happy to explain what the FIDO Alliance is and answer those questions. FIDO is different from other collaborations that have been spoken about, but there are similarities. What makes it different is that FIDO is not a payment-specific collaboration. Our focus is on authentication, and helping companies throughout the authentication ecosystem ensure that their implementations of authentication technology are safe and secure for consumers and for the companies relying on them.

When you think about the authentication landscape today, there is a lot of looking for that silver bullet. Everybody understands there are lots of problems in authentication, and a lot of people are running quickly toward the new silver bullet of biometrics. I am going to talk about the key principles FIDO lives by and says if you are going to move to biometrics or some other kind of authentication in a mobile device, make sure not to make the problem worse by following some of the same problems experienced with passwords.

Who is the FIDO Alliance? If you look at the board of directors, what you see is a true cross section of every type of company involved in authentication. Similar to some other collaborations, you see representations from many players in the payments landscape, but they are not here specifically only to focus on payments, but also to focus on access in any way to any personal or private data, some of which may or may not be financial. The

healthcare industry is also part of the FIDO Alliance and we are hoping it becomes an even broader opportunity. There is a lot of commitment across the technology and finance spaces in the FIDO Alliance.

What is the FIDO Alliance's mission? Many people have this image of a dog. Take that out of the picture completely. A lot of people also have this image that FIDO is a product. It is not a product. There is no profit in this equation. It is not a big database where all of the biometric prints sit. I have heard everything under the sun about, "Oh, you know, talk to FIDO about that," but that is not what FIDO is about. What FIDO is about is developing technology specifications that companies can implement across the spectrum. So you will see that it gets built into the handheld device itself, built into the servers on the relying party side and it employs this specification across the board with a certification process. There is an operating adoption program, so we have the whole marketing arm of the FIDO Alliance to ensure that this is truly getting adopted across the landscape. And then we are going to pursue formal standardization, as was talked about yesterday. Right now we really are just specifications until we go through some of the broader global standardization bodies.

As I mentioned before, the FIDO Alliance was formed to solve this ugly, ugly password problem. And in your world, it would probably be more PIN and authorization and things like that, but when you think about the whole ecosystem, everything comes back to these critical secrets—passwords, PINs, data, etc. We know we have this awful problem; we know what happens. You are living it every day. A lot of people try to solve for that problem by taking a different approach and saying, OK, how about going to one-time passcodes, and solving the problem that way. While one-time passcodes are certainly an improvement on passcodes, they certainly are not the ideal solution for various reasons many people have experienced themselves. They are not that user-friendly. You have to sit and wait for your little code to come. If it is a physical token that you have to use, and you have to type in a code, you end up with a key like a janitor's keychain with all the little tokens hanging off of it. It gets confusing for customers. Which code is this, and when am I getting it, and unfortunately, it is still phishable. We have seen in the last year that more and more of those things are getting phished as well as intercepted. So, one-time passcodes are not the answer. Passcodes are not the answer. What is the answer?

What the FIDO Alliance says is, “We need a new model, a new paradigm for how we view passwords, especially if we are going to move into this space where we are relying more on biometrics.” When you look at and try to analyze some of the key problems with passwords, there are consumer issues with, “I have to remember it, and it needs to be alphanumeric and include my gardener’s middle initial and I do not know what it is.” It is awful and everyone understands that. But when you look at the way it works, you have a consumer taking that very critical piece of data and sending it across the wire to a server. There is a lot of vulnerability. You can interrupt that online arrow any number of ways if you are a bad guy, or you can just target—no pun intended—the server. So when you look at the new paradigm, in many ways similar to tokenization, what it says is devalue all that data and turn it into a cryptographic key environment. What you are talking about there is that the consumer interacts with their device. This could be a mobile device or a laptop. You are interacting with that device and proving to it who you are using a biometric, PIN, or something else. And then that device generates a private key and stores it in the secure aspect of that device. That private key then speaks to a public key on the server side so then the authentication is really happening, the credential is really those keys and no longer the biometric. Instead of looking at biometrics as, oh, all I have to worry about if I am a big company like Bank of America and I want to use biometrics, I need to make sure that the false accept rate and the false reject rate are where I want them to be. Most banks are not in the business of understanding that business. That is not their core competency. But being able to say, OK, I have a key on my server, and it can only speak to this unique key on this device, we can certainly understand that a lot better. It actually takes a lot of pressure off making sure every single biometric is at the false accept rate that you need, and you can start to evaluate the risk you are using to determine how much security you really need out of this device.

When you look at what FIDO offers, it is a standard or a set of specifications that can solve for two different business or use cases. One is we want to get rid of the password and replace it with some sort of device-centered biometric. FIDO has a standard for that. Or, not all devices are going to have biometric capabilities, so how can I still use the FIDO standard? I can still keep my password environment, but instead of the one-time passcode I can layer on top of it a universal token. In some cases that is a physical token; in others it will be built into a device so it can be incorporated there.

When you look at the FIDO Alliance's key principles and you start to think about implementations across the board, if you follow these key principles, then you are closer to being in conformance with FIDO than if you did not. So, no third party in the protocol, no secrets on the server side. Think about the problems we have gotten ourselves into. To this point, it has been breach, breach, breach, breach because we have secrets that are breachable and we should not be so arrogant as to think we can perfectly secure all of that. Just like you have been saying about devaluing the data, do not take your favorite thing that you do not want someone to have, and leave it in a jewelry box for someone to break into. Only leave your crappy stuff that nobody wants in there. Leave nothing there that is worth taking and you will be in a much better position. Biometric data creep people out. They do not want it in the hands of big bad banks, others and government. They want to keep it close. So, keep it in the device, so it does not go anywhere and what happens to their biometric is between the consumer and the device. That means that if I am a bad guy and I want to remotely steal fingerprints, I have a lot of work to do. I have to fly to the United States and start stealing 2 million devices, instead of sitting in my hotel room in, we will not name the country, opening my laptop and starting to hack.

No linkability between services, no linkability between accounts. If I have a FIDO-certified device, and I will talk about what that means, and I enroll my device with PayPal, and then also with Google—just because Google and PayPal accept FIDO does not mean they share any information about you—it is completely separate. Look at what the FIDO Alliance has accomplished, similar to the collaborations we have talked about. The public specifications, you can go to the website today and pull off that specification. It was publicized in December and companies have been building to that. In 2014, we saw adoption by some key players, PayPal, Alibaba and Google. This is clearly a global group, not just a U.S.-focused group. Today, if you are a Google customer, sign up for two-factor verification, two-step verification, it will give you a choice. You can use a one-time password. It will send you the SMS, or you can go to Amazon and buy a little token. And you put it in your USB port and it functions as your second factor. You do not have to put in any codes. You just put it in your USB port. So, someone would have to get your password and your device because this token only works in that device. In 2015, we saw more momentum with Microsoft announcing that Windows 10 would support FIDO. Qualcomm has said their chips will now support FIDO in devices where they have

been placed. Google has expanded its use of the token to Google at Work. And NTT Docomo, the largest Japanese wireless carrier, has announced a whole line of FIDO-certified devices. There are a bunch of other companies that have gotten FIDO certified. And perhaps of most interest, it now is a public-private partnership because the government is joining the FIDO Alliance. The National Institute of Standards and Technology just joined, and the U.K. government just joined. So it is your turn to join, and ask me any questions that you have about the FIDO Alliance.

Mr. J. Williams: Any questions for Liz?

Mr. Horwedel: My question is that given the fact that we are about to see a huge increase in e-commerce fraud as a result of moving to EMV, and the merchants are going to bear almost all the associated costs, should we pay any attention to resurrecting 3D Secure, which was a very poorly designed product in the first place that resulted in gross abandonment of purchases during the process. I understand it has been redesigned. Should we go down that path, or can we expect something to materialize, or has it already materialized, that we should move to rather than fooling around anymore with 3D Secure?

Ms. Votaw: I cannot really comment on 3D Secure, but I can say that there are Web solutions as well as mobile device solutions that FIDO offers. As I mentioned, Microsoft's Windows 10 opportunity means that if you go on the new browser Microsoft is introducing—Microsoft Edge—when you interact with any of those companies on the Web, if any of them accept a FIDO authentication through Microsoft Windows, then you will be in a much better situation from a security perspective. I think the future is very bright for innovation and technology, and really what the FIDO Alliance is saying is go down all of those paths, but do it smart. Do it according to a standard that everyone can sign up for.

Mr. Horwedel: And correct me if I am wrong. You are also saying that you are focused in an open standards environment rather than a proprietary standards environment. Is that correct?

Ms. Votaw: Completely open source, yes. The only thing you pay for in this environment is if you want to say that you are FIDO certified, you go through certification and pay a small fee. And then to implement FIDO, it is open source, but there are vendors you can hire to do the implementation, so you can buy the server from the server vendor. If you are a

merchant, and you want to have an e-commerce site and be able to accept FIDO devices, you can hire a FIDO vendor or you can build it yourself. It is open source.

Mr. J. Williams: Thank you for the question. One thing that strikes me listening to the panelists is that to be successful in any of these collaborations, it is very important to define the scope and focus on those deliverables. How do you measure effectiveness or whether you have succeeded? Charles?

Mr. Bretz: That is a good question and I think there are a lot of metrics out there, and of course, more metrics that we could collect on those. It is a challenge for us on the cybersecurity side. You see these published numbers—\$10 billion are lost or \$1 billion are lost, and it is done by an estimate by some outside firm, and it is not really tallied where we would be audited and have audited numbers. Back to the card brands, they certainly can measure chip-to-chip transactions; they can measure the fraud as a percentage of payment volume and those types of things. We are going to have to look back to card brands. NACHA collects statistics in that area. What we are going to have to do is look to those folks in the payments area that collect that data. Certainly the Federal Reserve does a study every couple of years on the losses, and so those are the measurements I would want to go back to rather than the headlines we sometimes see in the trade press.

Mr. J. Williams: So you are looking at a financial metric?

Mr. Bretz: Right.

Mr. J. Williams: Nancy, what does the success look like for you?

Ms. O'Malley: The objective measures certainly are an important aspect, and that is why one of the essential things the PSTF felt was important to contribute was data on migration to EMV. We are getting ready also to launch surveys about utilization of tokenization as well as encryption because it is really the suite of these technologies that will work together to create a safer environment. Those are the objective things. But probably the more important things are the subjective things, the partnerships being built, the networking that is occurring to share thought leadership. FS-ISAC certainly does that in the cyberspace, but in the payment ecosystem that historically has not happened between competitors. Of course, we have to be very careful and monitor the space in which we do that, but in the security space, it probably is the easiest place for us to come together and

collaborate. So, we are measuring success by publication of thought leadership papers, the feedback we receive, the requests for more information and data, tasks from our executive committee, what we need to continue to do or tackle next. Those are what we are looking to as subjective measures of the progress being made and our success.

Mr. J. Williams: So it sounds like you are looking at the metrics and working that out, how they are evolving, to the things that you are doing to try and secure the rest of the payments system?

Ms. O'Malley: Absolutely.

Mr. J. Williams: Sandy?

Ms. Kennedy: We do not have specific metrics other than the same commitment we had from all the associations involved over an eight or nine month period. We had literally hundreds of hours of conference calls, in-person meetings, and that is the same commitment and involvement from both the retailers and the financial services and other players in the ecosystem. It speaks for itself that we had that kind of participation and that we have ongoing conversations, less formal perhaps, but ongoing partnerships and conversations that are occurring and understanding that we have a commitment to a shared customer that we need to protect.

Ms. Votaw: My answer is easy. Adoption. That is how it is measured. The more companies that say we are going to take the time and build security into our whole process, the more successful FIDO will be and the more likely it will be to spread across sectors beyond financial into healthcare and other areas that desperately need help, and consumer behavior. If consumers start to really adopt biometrics as a way of life, but feel comfortable about it and feel protected, then FIDO has been successful.

General Discussion

Role of Industry Collaboration in Payments System Security

Mr. J. Williams: Now I would like to open the questions to the audience.

Mr. Schmalz: One comment and a quick question for Liz Votaw. The comment is that the use of the certificate-based authentication mechanisms means you do not have to protect secrets on the server side. Did you mean that in the context of the biometric templates, or in the context of symmetric authentication mechanisms, which require secrets on both sides?

Ms. Votaw: I meant it in both cases. There are no biometric templates stored on the server side, it is an asymmetric key environment, and it is a public key that is stored on the server.

Mr. Schmalz: But the server has to have a public-private key paired to authenticate itself to the endpoint, so there is a secret protecting its private key. If that is compromised, you can do a man-in-the-middle attack, so it is equivalent to compromising secrets for a symmetric key system.

Ms. Votaw: There are going to be some vulnerabilities, yes, but it is certainly better than where we are today with passwords.

Mr. Schmalz: We do both, and you have to balance the advantages and disadvantages.

Ms. Votaw: Sure, and RSA is on the board of the Fast IDentity Online (FIDO) Alliance.

Mr. Schmalz: Yes. The other question is something that has been an issue with public key systems since their inception. There are a couple of issues. There is registration or provisioning of the certificates down to the endpoints, making sure that the owners really are who you think they are from the server side, and then there is the revocation question. So everybody is familiar with SSL (secure sockets layer), where the revocation issue

really has not been addressed, and many times there are issues with just client's auto authentication. Are you addressing the registration and the revocation questions?

Ms. Votaw: When you look at FIDO, the registration is trying to solve for the password problem, but this is a step in the right direction. It is not going to happen overnight. Everything is tied to whatever the trusted session is for the party that is employing it. When you go to register, you are only as sure that it is the person as you were before you implemented FIDO. You have to register it to your existing password structure. You have to be able to know. If you look at the registration process, you would go into a trusted session and then register for FIDO with your device. Everything is only as strong as the password, as long as we have passwords. They are still the start of that process. But when you look at things like what Microsoft is doing, where you are going to be able to create an identity on your Microsoft Windows 10 device, and then their passport would allow you to transport that as an identity into a line of business, you are starting to get to a passwordless environment.

Mr. Hamilton: Thank you very much. That was real interesting to get the different perspectives on collaboration and I am a true believer in industry collaboration. It is critical for success. One thing I worry about in trying to encourage industry collaboration in Australia is the problem of overlapping initiatives. There are many well-intentioned, well-thought-out attempts to solve industry problems which run across each other because you need to get the same group around the table over and over again to solve a slightly different problem. MasterCard, for example, is on all four of the groups we just talked about. This is understandable, it happens all the time. I am interested in the perspectives of the panel on how you manage that problem, that you can have so many different well-intentioned, great ideas that struggle for success because there are so many of them?

Mr. J. Williams: That is a great question Chris. I was at an EU cybersecurity workshop about two weeks ago and one of the challenges they had was trying to categorize what we mean by cybercrime, because if you talk about it as online security, or as e-fraud or e-commerce fraud, or potentially even theft where it is done by an electronic mechanism, or cyber-enabled fraud or theft, then it gets sent down a particular route within law enforcement. There are particular task teams looking at each topic. The result was

that if you called it cybersecurity it was everyone's problem. So how do you solve this problem?

Mr. Bretz: A couple of observations: The groups that execute will probably survive, and that execution, much of it is built on the people in the groups and on trust. You have different companies, different technologies involved. So the question is do they trust each other, can they work together, can they execute? People ask us why the Financial Services Information Sharing and Analysis Center (FS-ISAC) is so successful. It has taken us 14 years to build trust and the network of information sharing. Much of that is group dynamics and can you execute. The groups that execute probably will survive on the standards side. That is leadership; it is the passion of the people in the group that makes a difference. I do not think there is one answer.

Mr. J. Williams: Nancy, since MasterCard is one of your members in the Payments Security Task Force, do you have a perspective on overlapping the other collaboration efforts?

Ms. O'Malley: Yes, and I thank you for pointing out that we do support all these efforts. We spend a great deal of time ensuring that we understand the mission of the particular group and that it remains focused on that mission. When we formed the Payments Security Task Force, one of the first things the PSTF said was, as a collective steering group, we want to make sure we supplement the work that is being done, for example, by the EMV Migration Forum. We do not want to interfere with that, and maybe we tackle problems that particular forum has not been successful in tackling and add value in what we bring to the overall equation. Our goal was not necessarily to be the organization that survived beyond this particular market event. Our goal was to bring the power of those particular organizations, which represented 80 percent of the market on the issuing side, to bear, to advance the work of other organizations. It was supportive at the outset in what it hoped to accomplish. Now it has evolved further because bringing safety and security to the marketplace is not just about EMV. It is about other technologies that need to be brought to bear. As we bring EMV to the market, we also are working to advance adoption of these other technologies so that years hence we will really have what we can at least perceive today to be the most secure marketplace that we can build. That is entirely about collaboration because we cannot do it alone. We have to listen to and respect all the opinions of all of the players in the market, and the impacts

of any particular decision that might be made in one technology will have on their businesses. We have to do a much better job of bringing those constituencies together and working together. Sandy commented on some of that, and we absolutely embrace the importance of doing so.

Ms. Kennedy: Fear helped drive our collaboration. There had been significant finger pointing after the Target breach, and we felt that to attack this in a way that would be meaningful to Capitol Hill and the statehouses, we needed to do it together and collaboratively. Any time we can come together and find solutions as a payment ecosystem, it is always going to be better than when Congress tries to find those solutions. It was really almost a fear factor that drove the participation and the commitment and the results.

Mr. Horwedel: In keeping with what you were suggesting about bringing together these groups, is there a further opportunity in making this more of an international flavor? We are doing things in the United States that are counterproductive, like chip and choice. It creates seams between the markets; problems for consumers. It is ridiculous that we are doing that. Should we not have, for example, more of an international effort to get rid of these seams in our payments system and deal with security matters on an international basis so that fraud does not simply migrate to the United States?

Mr. J. Williams: A great question, one I certainly remember having discussions about with law enforcement agents who were saying if we were really successful in the U.K., we move all our fraud to France. I would not agree with that. I think that is the wrong thing to do. Nancy?

Ms. O'Malley: Taking an international approach is absolutely the right thing to do. There is no question about it that MasterCard, being a global company, brings that. We believe we bring that flavor increasingly to these conversations. And we are cognizant of our responsibility to do that. Certainly, others who participate in some of these forums with us, like our competitors, are global companies as well. In the context in which we operate as a payments ecosystem, we recently have been focused domestically, but there is a unique role that we should play in the global marketplace. We have the most significant emerging technology companies located in the United States. We have major payments networks. We have some of the largest banks in the world, and we have a very diverse and technology-accepting environment. All of which should contribute not only to our responsibility to advance the adoption of technologies, but also ultimately

to lead the way. We have obstacles in our way, but I am excited about some of the things we are doing collectively and collaboratively to overcome those obstacles. We are working more together than we have in the past. It is not perfect. There is a lot more work to do, but I think some of the work the Fed is doing is also going to be a key in allowing us to advance as leaders in the marketplace, which is a place the United States should be.

Mr. J. Williams: I agree. I think that is what we are seeing. Charles?

Mr. Bretz: I used to work for an international bank, and I had the pleasure of working with colleagues from about 15 countries. I realized that there are legacy payments systems in each of those countries, and legacy technology systems, in other words, telephone systems, the Internet. An international system is a good goal, but I do not think you can completely do away with all those legacy systems, whether it is a payment system of the United States or in another country. It takes a while for those things to coalesce. It is a worthy goal, but the more you try to get an international standard, the more you have some difficulties. Also, you have currency issues and capital controls in countries. Those types of things are complex.

Mr. Carlson: Looking to the future, say three years from now, after EMV has been implemented and some of the task force work has been done, what do you think is going to be the major focus of private sector collaboration? And there is an additional question to that. Are we organized sufficiently to address those issues?

Mr. J. Williams: Liz, can I direct that to you first? When we all have FIDO-enabled devices.

Ms. Votaw: We talk a lot about does FIDO exist in three years, or does it become so much a part of the ecosystem that it does not need to exist? From a FIDO perspective, whatever the technology is today it will have evolved in ways we cannot imagine three years from now. The pace is so crazy, and you need to have your eye on the ball about keeping the standards and keeping the principles. I think we will still be around in three years focusing on the same issue.

Mr. J. Williams: Sandy, what does your future look like?

Ms. Kennedy: Our partnership has concluded, but if the need arises, we certainly would be comfortable reaching out to the Financial Services Roundtable and the financial services industry again to look for those areas

of collaboration, especially as we work to provide a seamless environment for our customer, whether it is mobile, digital, or in-store. That is our key asset, our customer. If there are opportunities for us to remove challenges, work on challenges together, I certainly think we would move forward on that.

Ms. O'Malley: The Payments Security Task Force, like the Cybersecurity Partnership, was not designed to have an indefinite life. However, there is a real interest in continuing to tackle some of the new and emerging issues—the need for information, for education at the CEO level, in the board room and the cybersecurity space. As long as our membership continues to ask us to reconvene and tackle critical marketplace issues, we perceive that as the need that should be addressed and most likely we would continue to do so. These things will have a life because as technology advances, and unfortunately as fraudsters innovate, we will see an ongoing need to adapt and adopt and to accelerate our efforts. Speed is a big issue for our marketplace, and we have to find ways to move forward faster to move with the pace of our competition, the folks who want to commit crimes against us.

Mr. Bretz: It will be amazing how technology develops over the next two or three years. We do not know what the next cool payment technology is going to be, and somebody is working on that right now, or teams are working at that. It is going to come out, and then we will be reacting to that. How do we secure it? How do we put it on whatever device we are carrying? And on the criminal side, the same thing. They are very well-funded. They are making a lot of money right now. So we will be reacting to their innovation.

Mr. J. Williams: Hopefully we can turn off the tap of cash funding them, and then maybe they will go and do something else, or maybe not. Any questions from the audience? I have one that extends the last question. Assuming we are really, really successful, and we completely secure the card payments system, where are the fraudsters going to go next? Liz?

Ms. Votaw: That is like the stock market. If we knew that, we would all be much better off. I do not know. Where are they going to go? They are going to go wherever the weaknesses are. Wherever we are not is where they are going to go.

Mr. Bretz: A member I cannot identify said yesterday that their fraud on the RDFI (receiving depository financial institution) side for the ACH (automated clearinghouse) was up double this year. They shared that with some other members, saying, “Gosh, I do not know if our numbers are

that big, but we are seeing an increase.” And then we are seeing faster ACH payments coming to the United States and that it is going to create opportunities to reduce risk because we will know faster about that transaction—is it a good transaction or bad transaction. But we also are having a problem in the United States now with business email compromise, where wire transfers are being originated fraudulently. Fraudsters are tricking the business into sending a fraudulent wire. In the United States, most of those are going to Hong Kong and China, to Russian-speaking cybercriminals. But they are sending it through China. And you were saying in the U.K. what they are doing with faster ACH, they would send it to a U.K. bank and then they would use the faster payments, which would be like a fast ACH, to send them to multiple endpoints. If we have that same thing in the United States, we are going to have to build risk technologies to try to mitigate that.

Mr. J. Williams: Absolutely. There are necessary tools we do not currently have in our arsenal. In the U.K., we have seen an increase in fraud against direct debits. Account details of individual customers being provided to ordinary businesses, who then collect money. It is not for the individual, it is for the fraudster, and they are buying some goods or service. Unfortunately, it is on the rise. Typically, it takes about six months for a consumer to notice they have fraudulent transactions on their account.

Ms. O'Malley: Some things, certainly card not present will be the most immediate attack. The work that Liz and FIDO are doing is probably one of the most critical things we could be investing in right now, because we believe and have seen that one of the next waves of migration would be some sort of account takeover activity. Our concern is that although there have been attacks on databases where we have critical PII (personally identifiable information) data, they are spreading those attacks. And the purpose of obtaining personal information is for the takeover of an account. Some recent data breaches are in nontraditional spaces that we do not usually think about from a payments security perspective as being impactful on our business, but they absolutely can and will be. So how do we link those together? How do we understand who those criminal groups are? How do we understand the target, what they intend to do with that data, and then how do we inform our financial institutions to protect themselves? All of that is important work that the FS-ISAC does. Then there is the work that Liz and her team are doing to build solutions to provide better authentication methodologies for our financial institutions so they not only can authenticate at the time of either

provisioning a mobile device or opening an account, but also at the point of transaction. Those are important bodies of work that will contribute to solving what is likely to be the next wave of attack.

Mr. Bretz: I have a comment about card-not-present fraud. When EMV was implemented in Europe, some of the fraud shifted from card present, because counterfeit cards are difficult to create after EMV, to card not present. But Nancy's task force has recommended that you put in an EMV terminal. They are also stressing point-to-point encryption and tokenization. The combination of those three might protect the PAN (primary account number) even if there was malware on the system. The PAN might be encrypted or tokenized, so it would not be of value to the criminal, so they could not do card-not-present fraud. It will be interesting to see what happens in the United States with the combination of those technologies. Also, you mentioned surveys that you have done. It would be interesting to see how fast those payments systems are implemented, and I say a more secure system that would have EMV, point-to-point encryption and tokenization. And I know you are trying to track that. Some of the members I support are also trying to track that. It will be interesting to see over the next couple of years how fast that technology comes in.

Mr. J. Williams: So, Sandy, if we can solve your card problem, do you think the fraudsters will start trying to redirect your supplier payments?

Ms. Kennedy: We do not believe chip is the only solution. It is an interim step, but it is important that we are constantly evolving, looking for where the fraudsters are going and protecting our customers. They expect us to collaborate, work together and find those issues that can make them safer in the end. Who knows how we are going to be shopping in five years, with our Apple watch or our mobile devices, or who knows? But it is important that we stay steady and consistent in our drive for making sure the payments system is safe no matter how our customers choose to shop.

Mr. J. Williams: Before we wrap up, I would like to ask each panelist to leave us with a closing thought to take to our organizations and try to implement. Liz?

Ms. Votaw: Other than joining the FIDO Alliance, consumer behavior is what is going to drive pretty much everything. As companies start trying to solve for the security piece, we have to be thinking about the usability and consumer side in trying to find that balance between usability and security.

Do not assume consumers are going to change their behavior, because the model has not really changed for them. It only has changed for us. Keeping the consumer king will keep us all on the right path.

Mr. J. Williams: Consumer friction and consumer behavior. Sandy?

Ms. Kennedy: We have a shared enemy and a shared customer. The more we collaborate, the more we work together, the more we can trust each other on these big issues, the more successful we are going to be in protecting our customers.

Ms. O'Malley: I could not agree more. Some of these initiatives have clearly demonstrated the power of collaboration, and what we can do when we come together and agree on and move forward with agendas that advance safety and security. There is a global role for us as a marketplace that is equally important and we have to be mindful and respectful of that. We can achieve a great deal in a very short time if we put our minds to it.

Mr. Bretz: A little different thought. If and when you are attacked, do not feel alone. Rely on your colleagues within FS-ISAC, or other partner organizations, to help you with that. Share information about the attack and ask them for help. We have seen dramatic results when those attacks happen and people have asked for help and had a rapid response. That is my closing thought for the day.

Mr. J. Williams: Thank you. I will leave you with one thought of my own. When I was preparing for this panel, I was dictating notes into my iPhone, and as it got the information, it misread data “breaches” as data “britches.” I think that is a topic for a completely different conference. However, with the “Internet of Things,” and wearables becoming more and more important, who knows what will happen in 10 years? We will be talking about data breaches within your britches. Thank you.

Role of Government in Payments System Security

Moderator: Gordon Werkema

Mr. Werkema: I have a few opening remarks and then we will turn to our presenters. When the conference began, Governor Powell stated important goals of the Federal Reserve in retail payments: strong security, high public confidence and responsiveness to evolving threats. As we have heard throughout the last two days, private market incentives drive payment providers to work hard in securing payments. Our first session highlighted various features of the modern payments system that may make private sector efforts alone insufficient to attain a socially beneficial level of payments security. As you know, payments are processed in networks involving many participants, and that makes coordination vital to security. Recent trends add to the challenge. In the last 15 years, payment processing in the United States has become overwhelmingly electronic. In 2000, just over 40 percent of noncash retail payments were initiated and processed electronically. In 2012, 85 percent were initiated electronically, but virtually 100 percent were ultimately processed electronically. Endpoints where payments can be made are exploding in the United States and throughout the globe. Merchants that accept card payments in the United States are above 10 million. Access to the Internet in 2013 witnessed 116 million households, and interestingly 64 percent used tablet computers. Nonbanks have been the leaders in developing new methods of making payments, especially in the online and mobile payment areas. E-commerce sales reached \$75 billion in the first quarter 2015, for a record 7 percent of total retail sales. Nonbank payment providers set a record for startup funding in 2014 at \$2.23 billion; but with \$720 million in startup funding in the first quarter of 2015 alone, that record will likely be broken this year.

While these are U.S. trends, we believe they serve to illustrate how challenging securing payments and transaction data more broadly has become. As a consequence, there may be room for enhanced public policy toward security.

This final session will explore the role government may take in promoting payments security. So, contributing to our discussion today, I would like to introduce our panelists. We have Chrissanthos Tsiliberdis, and he says I can call him Chris. He is a senior market infrastructure expert at the European Central Bank (ECB). He is responsible for operational risk oversight and policy issues. Importantly, he was involved in drafting the Eurosystem oversight policies on business continuity for systemically important payments systems, and he has represented the ECB and various working groups including those involving cyberresiliency. Next to him is Coen Voormeulen, director of the Cash and Payments Division at De Nederlandsche Bank. He importantly is co-chair of the Bank for International Settlements Working Group for Cyber Resilience. Lastly, we have Anjan Mukherjee, counselor to the secretary and deputy assistant secretary for financial institutions at the U.S. Department of the Treasury. Among his roles, he oversees the Office of Financial Institution Policy, the Office of Critical Infrastructure Protection and the Federal Insurance Office.

In their respective roles, these three panelists have been involved in policy initiatives related to deterring payment fraud and/or improving cybersecurity. We hope this session sparks questions and dialogue. Initially, I am going to turn to Chris. He is going to give initial remarks, and then we will ask some clarifying questions and then move on to the other panelists.

Mr. Tsiliberdis: Good morning, everybody. I would like to thank the Federal Reserve Bank of Kansas City for inviting the European Central Bank to express the views of the Eurosystem at this conference.

The main objective of the central banks in Europe is to ensure that the financial market infrastructures are safe and efficient, which is a precondition for doing three things. First, we would like to contribute to financial stability. Second, we would like to implement monetary policy. And third, we want to ensure and maintain public confidence in the currency. When we look into financial market infrastructure, we do not oversee differently the large-value payment systems and the retail payments systems. For that reason, maintaining public confidence in the retail payment systems and retail payment instruments is very important.

To maintain public confidence, the task for the central banks and the other regulators is threefold. It is to keep their approaches flexible enough to accommodate the pace of innovation, to ensure fair competition among

actors and to require that service providers implement adequate minimum security requirements. Accordingly, we have been actively monitoring what the market has been doing all these years. Initially, we had a very passive role in this, monitoring the market initiatives and how they were doing in order to sustain the efficiency and safety of the instruments they were providing to the market.

But we realized this was not very successful in some cases. So, we stepped in and started introducing new standards. We started introducing new recommendations, for example for card payments schemes in 2008 and afterwards for payments instruments, like SEPA direct debit and SEPA credit transfer. Then, our oversight standards for retail payment instruments looked into various areas of risk management such as the financial risks information provided by the actors of the instrument. We looked into aspects of security of the retail payment instruments, operational ability and business continuity. We provided some recommendations concerning the governance arrangements for the different retail payment instruments, as well as about the management for financial risks regarding clearing and settlement, which is behind all these instruments and schemes. We also took an oversight approach to ensure a level playing field was maintained for all the retail payment systems. We developed assessment guides, and these guides were used by the central banks as the driving tool to ensure this.

Currently, we are implementing some regulations to ensure that the previously non-legally binding recommendations are now legally binding. That means that card payment schemes and providers of the retail payment instruments will do what we identified in some of the areas. This is where we actually have implemented the Bank for International Settlements' Principles for Financial Market Infrastructures (PFMI). This is an ECB regulation now, applicable to all systemically important payment systems. Some regulations are applicable to retail payment systems, and some are also applicable to less prominent retail payment systems. Because of this, we also have started a number of assessments. We are at the end of the grace period for large value payment systems and soon the retail payment systems will deliver to us the self-assessments against the standards. Additionally, we have a number of assessments in process concerning oversight of payment schemes, especially on cards where we want to emphasize evidence of the security of Internet payments and on the European direct debit scheme, which has been active for two years.

Concerning retail payment instruments, the European Commission is revising the Payment Services Directive, which aims to introduce regulation for new types of payment services, such as payment initiation and account information services offered by third-party providers. We realized that some new entrants in these markets are afraid that this new regulation will be regarded as a warning, but we believe that the sooner new entrants become regulated, the sooner we can assure they are participating fairly in the payment industry and providing these tools efficiently.

When we saw some cases where the market did not provide what we were expecting, we stepped in as central banks and developed our own retail payment systems. This was the case for some jurisdictions in the euro area where they provided the retail payment systems and we have developed expectations further by also making them systemically important.

Another area where we very actively work is in promoting cooperation between the various sectors. The cooperation is done first among the various national authorities. As you know, we have different authorities in the EU; banking supervisors, securities regulators, and different authorities, so we want to ensure that they all are actively involved. For that reason, we have a number of Eurosystem and ECB related committees. And all these committees work together to define the right standards and principles. For example, we were actively involved in the creation of the SecuRe Pay Forum. This forum brings together overseers from central banks, supervisors, regulators and other euro authorities, plus law enforcement agencies active in the euro area. We discuss and focus on payment security.

In addition, we recently established the European Retail Payments Board. There are many participants from the private sector and various EU authorities. The main focus is to foster standardization and market integration in the EU. Of course, the more choices we have the more responsibility, creating more expectations for the market. For that reason, we want to ensure that what we have developed has been accurately implemented by the central banks and that we have done what has been mandated to us as overseers of these infrastructures.

Further, we have cooperation between the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), which are very important in terms of developing standards and new policies for cybersecurity and cyberresilience. We

are awaiting the outcome of the CPMI-IOSCO's work and in the interim are working on a number of initiatives concerning retail payments. So, we are working with various authorities to establish a reporting collaboration scheme for sharing major incidents and information about threats. We also have established forums and task forces for discussing how to improve secure communication and certification, and third-party access to payments accounts. This also will be covered by the Revised Payment Systems Directive. Because there are different regulations and standards, we would like to ensure that all the standards are harmonized among the different regulators in the euro area, and if possible, globally.

In that field, we also would like to ensure that we will establish a new incident reporting scheme, which will have to be done in cooperation with other European authorities, like the banking supervisors. This will be very interesting, once we develop the technology we agree on with them. And yesterday, you heard about our work on fraud management and fraud reports, and we have been actively involved in that field as well.

Finally, we are constantly analyzing various developments. We are in close collaboration with the different market stakeholders. We organize regular conferences on the extent of use with all the different actors in the European landscape. For that reason, we do our analysis before we make our recommendations to our governing bodies.

Mr. Werkema: Thank you. Do any clarifying questions come immediately to mind? We will move to our next presenter, Coen Voormeulen.

Mr. Voormeulen: Good morning, everybody. We have talked a lot about retail fraud, tokenization and passwords. It is very interesting, but I would like to shift the focus. What if the big players—Visa, MasterCard, Fedwire—were attacked by cybercriminals, maybe not to steal money but to destabilize the system. That is a different ballgame. That may even hurt the confidence in the whole financial system, and thus have systemic consequences. That is the same as if the wholesale market would be hurt. Jonathan Williams asked what will be the next step if the payments chain is fully secure. Maybe the wholesale market will be the next target. Then there will be systemic consequences, and that is a big concern for me as an overseer. Therefore, the financial market infrastructures (FMI) are the focus of the group that I am chairing, the Working Group on the Cyber Resilience of CPMI and IOSCO. Those are two international committees for central banks and for market supervisors dealing with standards of the payments

and security sector. It is set up with about 20 countries. What we try to do is to publish guidance notes, one of which is planned to be published for public consultation this November. This guidance note is one step deeper than the existing principles for financial market infrastructures, the PFMI, which was published in 2012, and is the bible for overseers on how to look at FMIs in terms of business continuity, operational risk, legal risk, business risks, (everything ... risk management in general).

In that document, which took a long time to publish, not that much is said about cyber. Therefore, this Working Group on Cyber Resilience was created to go one step further and to see what we can do there. I can talk for hours about that guidance note, but instead I will highlight a few points I consider important.

First, I would say cyber goes much further than information technology (IT). A lot of the discussion in the last one and a half days has been about IT. But when we look at financial market infrastructures, there are several things that maybe are more important than IT. For instance: people. As we know, many attacks on institutions start with social engineering, where people click on malware in an email, in an attachment in an email, and then when the hacker is in, it can go into that organization's critical systems. It is very important that the people in an organization have a clear picture of what they need to do to protect the organization against cybercriminals. So, cyber is also involved in such things like culture. What are you going to do if somebody did something on the Internet of which he thinks, "Oh, that was a mistake." Are you going to punish him? He probably will not mention it then. It is very important to have a culture where people will be open to saying, "Oh, something has gone wrong; I will say it to those who can maybe solve it." It is in line with the saying, "When you see something, say something." When you see that you have made a mistake, say it. But it is not so easy.

Another element is processes. If an institution wants to launch a new product, service or tool, traditionally we like to ask whether it delivers the service; does it do it effectively; is it at low cost; is it speedy enough, user-friendly enough? But we do not always ask the question, if we introduce this new service, what about the whole cyberresiliency profile of my institution? Does it add or diminish risks? That is also important to consider when new services, products or tools are launched.

Finally, an element I think is necessary to stress is communication or collaboration, especially if you look at FMIs. It is actually relevant for every institution. You are never on your own. You are part of an ecosystem that is specifically relevant for FMIs where payments transactions or securities transactions go through many players. So, it is important to communicate with those players not just when there is a crisis. Also, not just to exchange information in advance, what the Financial Services Information Sharing and Analysis Center (FS-ISAC) does, but also, maybe if an institution will be attacked in terms of its integrity. So, if the systems will be corrupted and you need, for instance, to resume after such an attack, you need clean information to restart. Where do you get that clean information? Maybe from your customers, or from third parties, or critical service providers. It is good to have arrangements with those parties in advance, so that after an attack, you can resume quickly.

What about top management? Unfortunately, we also discovered that while top management has a very important role in making sure that their institution's cyberresiliency is at high standards, most in top management are not digital natives. They have gray hair like me, and they consider cyberissues difficult to grasp. It is not their cup of tea. The inclination is to leave it to the IT department. That is not a good choice because the IT department is technically focused, and we need to think about more than that. So, the role of top management to steer a proper cyberresiliency policy needs to be stressed. Unfortunately, it is not always as we would like to see it.

My last point is about what we see now as the biggest risk. I would say that it is the recovery from a successful integrity attack. If an FMI is successfully attacked, and its systems are corrupted, the data are corrupted, a plus is a minus, or three or six zeroes would be behind every transaction. That is really a headache scenario, and what we see is that FMIs in many cases have put a lot of effort in preventive mechanisms; also in the detection of possible cyberattacks, but still a bit less in what to do afterward, how to resume your operations in a safe way. If you just resume, but you have the same vulnerability as before, that is not the best world. You have to resume in a safe way. We clearly see that more attention to that would be very useful, especially because in these PFMI, there is one requirement that says that after an incident—and not specifically mentioned as cyber, but it is also relevant for cyber—you should be back in operation in two hours. There is a two-hour recovery time objective. When we talk to FMIs

about that, they say, “Wow, that is not possible with an integrity attack. It may take even much more than two hours to analyze what is the problem, let alone to get back into operation.” I understand that, but that is thinking in the old framework because these kinds of attacks can happen, and we cannot afford systemically relevant FMIs to take two days to get back into business because in the meantime the financial system might already have been broken down. If you say, “Well, that is too complex to make sure that I am back in business in two hours,” then I think it is necessary to widen the perspective.

Nowadays, many FMIs have a hot standby, and maybe even two hot standbys, in remote locations. That is very useful for many circumstances, but it is not useful if you have an integrity attack, because then you freely copy the malware to your hot standby. That is convenient for the attacker. One possible solution is to have a different standby. It does not have to be in a different location, but in terms of different software, different hardware, maybe different people who made it. In the aviation industry, that is sometimes how they increase security in planes. This might be a solution by thinking in a different framework. FMIs say, “Oh, but that is too expensive.” I think it is not, actually. There are central banks who have this because you can do it in a way that may not be a 100-percent copy of your primary system, but in a way that at least the critical transactions can flow further and maybe in a slightly degraded way, but at least in such a way that the financial system does not collapse.

Again, as I said, we planned to have this guidance note ready for publication in November. We have a two-month public consultation period, so the whole world is invited to react and we are curious what reactions will come. If this guidance note is then published in spring next year, then it is up to individual jurisdictions to lead that into domestic legislation if they want. Then, I think we as a cyberresiliency group are a very small piece of making the world slightly safer.

Mr. Werkema: Thank you. You have shared about systemically important infrastructures and a little about the process you went through. Maybe you could elaborate on that. But then also give us some indication of where there are parallels for retail payments. Obviously, we have talked a lot about retail payments over the last day or so.

Mr. Voormeulen: Yes. The PFMI; they have a clearly defined audience that includes systemically relevant payments systems. We do not want to

change that audience, but I would say we invite countries to apply the same, but in a risk-based manner, to other financial market infrastructures such as not so systemically relevant retail payments. Maybe you can be a bit more relaxed there. But the principles themselves are similarly relevant, and maybe you can, as I said, be slightly more relaxed about how strongly you would implement all the principles. But I would definitely recommend making the retail systems as resilient as possible in this way.

Mr. Werkema: Is there agreement at this point in your group on these six principles?

Mr. Voormeulen: These are just my reflections. The paper is set up a bit differently. It partly follows the National Institute of Standards and Technology (NIST) system to connect it to what is already well-known in the market, and we stress certain things around it. But it is my reflection; I do not think there will be a lot of disagreement in the group.

Mr. Werkema: Good, thank you very much. We will turn to our third panelist now. Anjan.

Mr. Mukherjee: Thanks for the opportunity to address you all today. At the Treasury Department, we are very focused in areas of the “greatest risk.” Obviously, we are all sitting here today because our payments systems nationally and internationally handle staggering sums of money. Just in the Federal Reserve System through the 12 banks, there is something like \$4 trillion per day that goes through the system, which is a quarter of annual GDP in the United States. And the total volume of payment activity annually is approaching \$200 trillion, which is a staggering sum. So, we tend to go where the big dollars are in terms of risk focus. We note that much of the architecture that underlies the payment systems, that supports this massive volume of activity, is legacy in nature and subject to the rapid technological change that we see today—the rise in mobile computing, the greater ubiquity of high speed networks, ever accelerating transaction processing speeds. And so the combination of the legacy systems with a time of rapid technological change not only means that it is an exciting time in the world of payments in that some of these innovations may fundamentally change the architecture of the payments systems as we look to the future, but it also means that there is a need to be extraordinarily cautious. When you have this sort of combination come together, the underbelly of the rapid acceleration is the ever-increasing technological threats as well. The payments system, as I think of it, was initially built for connectivity, not for

security. So, we pay real attention to cybersecurity threats. It is an issue of real importance to us at Treasury, obviously the nation as a whole. Part of what I do is oversee the Office of Critical Infrastructure Protection, which among other things has the responsibility for monitoring and facilitating the protection of critical infrastructure in the nation's financial services industry, which includes our wholesale payments systems. We want to also ensure that the retail payments systems have the level of security needed to protect the work efficiently and protect consumers' private information.

We remain vigilant because it does not take much to imagine an attack on a wholesale system that could be crippling, as Coen says, and affect consumer confidence. And on the retail side, we are already well aware of some of the breach activity that has led to divulging private information, which we are trying to prevent. In our role as Treasury and sort of an organizer in the executive branch around the financial sector, we operate on multiple levels. We try to coordinate and facilitate administrative executive level activity as well as legislation on the former to address some of these issues. You may have seen recent executive orders that the president has issued on some of these issues. One thing we did in October, was an executive order around retail payments, accelerating the security of retail payments where we as a government felt that we had almost a priming-the-pump type function when it comes to retail security. We announced our Buy Secure Initiative, which is an initiative to roll out EMV chip and PIN technology in the existing and future government card network, and also to replace all the retail terminals in the government system to make them compatible with EMV as a way to harness the government's purchasing power. You have recently seen a sanctions executive order that is targeted at malicious cyberactors where the Treasury Department will use its sanctions authority to specifically deter cyberattacks. And then at the beginning of the year, we helped formulate and coordinate the administration's legislative proposals on cybersecurity, which looked to facilitate information sharing and data breach notification and a few other things that we can talk a little more about.

So having set that stage, I want to focus these opening comments on a few areas where I think government and the private sector can work effectively together to promote a more reliable, secure and resilient payment system, both on the wholesale and retail sides. In fact, in some ways at Treasury our entire framework for dealing with cybersecurity issues roughly falls into the following categories. First, it is promoting best practices and baseline

protections; second, is sharing threat information; and third is improving response and recovery planning. We have heard about elements of each of those throughout the conference and earlier this morning, but I wanted to talk about them in more detail.

First, on best practices: These are the policies, procedures and other controls that an organization will adopt to prevent penetration of their networks by malicious actors. As Coen just mentioned, the NIST framework for improving critical infrastructure cybersecurity is one of the best examples of a set of practices. The core five functions are identify, protect, detect, respond and recover. This is a tool to help systematize your organizational cybersecurity. If you are not using NIST framework, you should be. Probably everyone in this room is well familiar with it. NIST is working on evolving the framework, but I would encourage you all to do the same. It is really a foundational starting point to think about, not only the narrow issue of cybersecurity risk, but really the broader issue of risk management and organizational resiliency. So I hope you build upon this framework to more deeply embed organizational risk management into your business strategy.

As for baseline protections, there is a lot of interesting technology that is evolving. We have heard about some of that over the course of this conference. I would simply encourage everyone to examine moving toward more state-of-the-art security solutions; advancements one ought to embrace. Whether it is around encryption and authentication solutions, making sure everyone is completely compliant with ISO 20022 standards, moving to more of a credit push as opposed to a debit pull model as we think about money transfer, we think there are some important technological advancements. We do not endorse any one of them, but we encourage you all to explore them more carefully and embrace the ones that make sense for your organizations.

Next, I would like to highlight the importance of information sharing in this arena. I think this is one of our most potent tools to counter malicious cyberactivity. To reduce risk over time, we have to understand the threats we face. Many times the best way to do this is by looking at other entities and sharing information—the threats that someone else faces, that your organization faces, other entities could benefit from learning about. The malicious cyberactors are sharing information and tools all the time. We on the government side and the public and private sectors together should be doing the same thing, obviously in a way that protects privacy and business reputation.

As I mentioned, in January the president sent an information-sharing legislative proposal to Congress that included things like liability protections to encourage companies to share cyberthreat information, and to encourage industries to set up information sharing and analysis organizations (ISAOs), and we are firmly behind that. I hope we can talk some today about the extent to which major payments system stakeholders are engaged in such information sharing, including through our friends at the FS-ISAC that we heard from this morning.

The last area I want to address relates to response and recovery. Obviously, there is no such thing as complete security. So we really have to do everything we can to prevent the initial attack, but also to be prepared when an attack occurs. It is important for us to maintain both national and organizational incident response plans that make your incident response process much more effective, predictable and efficient. We encourage all organizations we deal with to have very strong incident response plans in place, and to exercise them. Exercising these plans really helps senior management, the security teams, external stakeholders, all the various constituents to be comfortable with their particular roles and responsibilities when and if an attack occurs. So I would just ask a few questions around this: When was the last time you exercised your incident response plan? How were your third-party service providers pulled into this effort, because we think that is very important when thinking about this question. How did you include your external stakeholders, such as law enforcement or your regulator, if that is appropriate, or Treasury? These are just some questions to consider.

I will close by emphasizing that this cybersecurity issue is really all about collaboration—public and private collaboration. There is no single government agency that has sole responsibility over this issue. So we collaborate within the government, and it is critically important. This is an issue that is cross-cutting, so it is incumbent upon us to collaborate among the private and the public sectors. Adopting these baseline protections and best practices, sharing threat information, improving our response and recovery posture is critical. All of it will benefit from collaboration between public and private, and ultimately that is to the benefit of protecting the integrity of our payments systems, which nationally and internationally are a real resource.

Mr. Werkema: Thank you, Anjan. Any clarifying questions? OK, perhaps I will give a question about financial market infrastructure to all three of you. Obviously, the countries represented are key players. Talk about

communication and coordination between key financial market infrastructures on these issues of resiliency and cybersecurity.

Mr. Tsiliberdis: In Europe we are organizing a crisis communication test where we have invited the major payments infrastructures and a number of banks to participate. Our objective is to test the crisis communications arrangements and also how they will react in such a cybersecurity event. We place a lot of emphasis on this. For that reason, we have established a specialized task force to implement this procedure and this exercise. Until now, we have realized that in the euro area, we had mainly conducted exercises organized by the systems, but nothing was done in terms of marketwide exercises. So this is one of the first steps that we are doing in this area.

We also are promoting information sharing between the different FMIs. That is why as I mentioned there is a new specific process between the SecuRe Pay Forum and other forums where we try to bring together the different regulators and law enforcement agencies to exchange information about cybersecurity threats and other risks or incidents, which are occurring on a daily basis in our infrastructures.

Mr. Voormeulen: The interesting thing in the Working Group on Cyber Resilience is that the optimal way of coordination is very different from country to country not just because of different legal setups, but also different historical and cultural habits. There are countries where the regulator needs to push cooperation. Otherwise, it does not come across. There are also countries where if the regulator steps in, then the coordination stops. The markets themselves do that much better. But I would say that in any case, it is important within your own cultural environment to stimulate coordination by many different things. The CERTs were mentioned several times. That is on a very practical level. The FS-ISAC was mentioned. You also can do crisis management exercises nationwide. That is what we do in the Netherlands. For the last three years, these crisis management exercises always have been about cyber, and not about any physical accident. We are now trying to expand that. So far, it is in the financial sector, so all players are there. But we are trying now to expand it to the energy and telecommunications sectors because those are crucial players also for the financial sectors. Without telecommunication, we cannot do a lot anymore. So we have our own, we call it FI-ISAC, but essentially it is the same thing. But for me, the biggest struggle is how to get it off the ground internationally because the borders are not relevant for attackers. So in the end, it is all

about international issues. But it is very difficult to set up an international forum for official collaboration. This Working Group is a little tiny effort to do that. But maybe an option is what we heard this morning, the FS-ISAC is expanding internationally because the institutions that are involved are international institutions. They have business in other countries as well. So maybe that is also a good way to make a step forward.

Mr. Mukherjee: Yes. I was going to underscore what Coen said at the very end, which is that challenges are around international coordination. When we look at FMIs, even within a single FMI, there are barriers to information sharing due to security clearances or confidentiality agreements. That is within the FMI entity. Now if it is a global FMI, you have the home authority, you have the host authority, and these sometimes are conflicting and I am not sure we have done enough yet to coordinate across border. So we support the work at CPMI-IOSCO around this and we have input there. I think that is where we will start the lead. I will say that we are starting to create exercises. We are very supportive of the crisis management group efforts and the exercise that Coen mentions, that is often done on a national level. I think the next step for us is to try to tackle that on an international level and deal with the cross-border issues. But we will get there. We are establishing not on FMI specifically, but more broadly, an exercise that the United States will do with the U.K. either later this year or early next year. I view that as a first step toward more of an international exercising regime that we can utilize to test these questions around FMIs in particular.

General Discussion

Role of Government in Payments System Security

Mr. Werkema: Thank you. Have the responses spurred any questions from our conference participants?

Ms. George: I want to thank each panelist for the perspective you brought on the issues we have been discussing for the last day and a half. Coen, you made a comment that I found interesting, which is we tend to think about technology when we focus on these issues instead of the importance of culture. My question for each of you, but I am happy to hear Coen elaborate on this, is what role do you think public authorities play in influencing culture? Is that primarily through education, regulation? What, in your experience, would a public authority bring to that?

Mr. Voormeulen: That is a difficult one. What I can imagine is that what helps best is to make people aware of it. We bring parties together, including a security company in the Netherlands called Fox-IT, which is very experienced. We bring them together to talk, to let *them* talk, to share these kinds of things with financial institutions and financial market infrastructures. Then, when the federal institutions hear it, they probably recognize something of it and can apply it. But you cannot impose cultural things. That is the difficult thing. The only thing possible is to make everybody aware by sharing practices.

Mr. Mukherjee: What I could add is that we find it is very difficult to prescribe culture. As Coen said, one way we handle this is by talking about it, but also by framing our output, not narrowly in cybersecurity per se, but more about enterprise risk management. So, when we encourage certain frameworks, like the National Institute of Standards and Technology (NIST) framework, or we engage with the private sector on cyber and we talk about it, it really is more about organizational and risk resiliency, overall business continuity, and we talk a lot about governance in that

context. There is no precise way to get a culture necessarily, but by framing the issues, the questions, and then the solutions that we would encourage in a broader milieu and with governance as an important part of that, that is how we indirectly try to get at it.

Mr. Tsiliberdis: What we emphasize is trust. We try to build trust among the different participants. We want to assure them that by building on this trust among themselves, they will be able to adopt technologies that will make them compatible, not enter into competitive fields. We try to help them see how this communication can be done from all the different actors by using technologies which are interoperable.

Mr. Santhana: I have a question for Anjan. We work a lot with federal and state governments. We find there is a big difference in terms of cybersecurity, enterprise, fraud management and even in the payments environment, payments modernization. There seems to be no set standard, no task force that helps pull the various state government entities to follow what the federal government is trying to do. Is there any initiative, anything going on now that you can share?

Mr. Mukherjee: It is a tricky one because states are independent. Each has its own, as you know in dealing with them, IT network and system and that legacy of independence. We have very much noted the issue you have outlined. There is no specific broad initiative, to directly answer your question, in the works to address this issue for many reasons. There are impediments in place for the federal government to try to standardize this issue or approach it at the state level. We are limited in what we can do, but we can talk about it. We have convened with certain leaders in state government to discuss the issue. We encourage state governments to join the Financial Services Information Sharing Analysis Center (FS-ISAC). But this is really more of a moral-suasion process, where we try to rope them into our effort, make them understand how we are approaching the issue and encourage them to try to look at it the same way.

Ms. Fine: All of you in your remarks touched in one way or another on both strategies of collaboration and moral suasion, best practices, education, as well as regulation, legislative approaches. I am wondering if you can speak about that balance, and where you found regulation to be most effective or necessary to preserve the safety of the system versus the other strategies you have talked about.

Mr. Voormeulen: Again, That is a difficult point because it is a balancing act. One characteristic of cyberresilience is that when you go deeper into the technicalities, everything you would put into legislation probably will be outdated before it is out. You need to be more high level in legislation to make sure it is still relevant next year and the year after because of the quick developments in cyberattacks. That makes best practices the most effective way in the short term to pass on to all the relevant parties, because they can be updated relatively quickly. But at the same time, a legislative framework that stays high level but aims at the goals and not how to get there can be very useful to exchanging these best practices.

Mr. Mukherjee: Yes, I would say these various efforts are complementary. More of all is better. There are situations where there is some potential conflict, but generally we think those are manageable and relatively minor. To take information sharing as an example, Treasury just joined FS-ISAC. We encourage financial institutions to join FS-ISAC, which has something like 5,500 members. The financial services industry is well out ahead with this ethos of information sharing, as evidenced by the success of FS-ISAC. Even though we are Treasury and the government, we promote adoption of this model by other industries—healthcare, energy and so on. But if you look at the president’s legislation on information sharing, it is wholly consistent with that sort of non-legislative approach that we have taken and it is just meant to provide additional impetus. As Coen just said, it is not technical, it is not detailed. It is meant to be a broader framework. In some ways, we are already working in that framework without the legislation, but we think the legislation has some very important elements that will accelerate what we are doing through liability protections, and other things, that will encourage not just the financial services industry, but participants in other industries, to adopt an aggressive information sharing regime.

So, I think that there is not necessarily, kind of the way you framed it, a conflict. We think these are complementary and more is better.

Mr. Tsiliberdis: I would like to add that the reason we move from moral suasion to regulation is because we have seen that some entities were not fast enough in implementing some of the policies, some of the recommendations, some of the requirements that we have highlighted with the previously non-binding recommendations that we were giving to them. So, to establish, to raise the bar in terms of efficiency and security, we have decided within the euro area and the Eurosystem, to convert some

specific recommendations into regulations. This is what we have done for the large-value payments systems and what we also are doing with the retail payments systems. Soon we will be doing this with the retail payment instruments, with the Payment Systems Directive once it comes into force, with other recommendations that will be issued by the European Banking Association Authority in the field of retail payment instruments.

Mr. Werkema: If I could just follow up on that, Chris. So, your framework had moral suasion, regulation, but then you also addressed the operate aspect with the European Central Bank (ECB). So, what would lead the ECB to stand up or enhance capability on the operate side versus collaboration, coordination, moral suasion, and regulation? What would lead to an operator capacity?

Mr. Tsiliberdis: As you mentioned, the area the ECB mainly has stepped in was the large value payments systems. And last Monday we went live with a new security infrastructure. It is where we want to ensure that services that are critical and important in the euro area, and for which we do not see the solution is already available in the market, then, in that case, we try to step in and implement these solutions. Sometimes of course, we will see some kind of reaction from a service provider that they know we are entering that field and ask why we are implementing something. But this is because we want to ensure that the level of service provided to the citizens and various financial institutions is appropriate. For that reason, we step in as operators for these specific systems. We have not done it yet. But in terms of the ECB in the telepayment systems or our telepayment instruments, I know the central banks in the euro area, which are active in this field, have implemented their own solutions.

Mr. Werkema: At the ECB level, your focus is on wholesale systemic systems?

Mr. Tsiliberdis: Yes.

Mr. Werkema: Other questions?

Mr. Moore: You all were talking primarily about public sector initiatives to improve payment system security, and each involved engaging the private sector. But this morning, we heard about several initiatives that were initiated and led by the private sector, and I am wondering what role, if any, do you think public authorities have in supporting or engaging with these private sector led initiatives?

Mr. Mukherjee: Maybe I can take that one, and maybe I will shift a bit the answer, to not answer your question specifically but to talk about a different scenario, which is where the public sector has created its own programs and initiatives, divorced from the private sector as a way to encourage objectives here. I mentioned one in my opening remarks, which was an executive order the president issued in October 2014. It is the Buy Secure Initiative, which has many elements. One is to move all government-issued cards to EMV technology. This is a way to harness the government's purchasing power to try to drive and encourage change and enhance technology in our system. If you look at recipients of federal benefits who are unbanked, the idea would be to populate prepaid cards with their benefits and the program we have set up is called Direct Express. It has about 2.5 million people on it. Those cards are populated with about \$2 billion worth of benefits every month. We as a government, independent of what the private sector is doing, have decided to encourage—and we talked during this conference about how the United States is far behind on EMV chip and PIN—to prime the pump in that way. Similarly, all of the government's payment card terminals will be upgraded. There are about 3,200 terminals across 52 different agencies. Our target is by the end of September of this year to have all those terminals upgraded. We are on target. We are finishing phase one with about 19 agencies, and there are almost 120 million annual transactions that go through that network. By the way, that hardware also will be near-field-communication (NFC) enabled. So, eventually the Apple Pay, Samsung Pay and Google Wallets of the world could—not that they will work day one—but could work because the hardware at least will be enabled to do that. So, it is not exactly what you asked, but I think it was important not only to talk about the private sector initiatives, but the fact that there are entirely public sector initiatives that also are meant to accelerate the pace of improving the security of our payments system.

Mr. Voormeulen: Maybe I can mention one example. In the Netherlands, we have a big group, a Retail Payments Board, which is chaired by the central bank. That is a broad group in terms of banks that are represented, retailers, consumers, but also disability awareness organizations for instance that have an interest in how user-friendly or what kind of retail payment devices are used. There are all kinds of sectors, with about 30–40 people around the table. Whenever there is an initiative or the start of an initiative in the private sector, it will come across that table. What we do then is to try to stimulate it, help it, sometimes a private sector initiative

needs competitors around the table. They find it difficult to agree on how to take it a step further, and then they need a neutral party, and then we can step in as a central bank or as this more societal organization to take the initiative further. So, everything more or less comes together on that table, and can be moved ahead in the best possible way.

Mr. Tsiliberdis: And just to complement what they have in the Netherlands. At the European level, we also have a Retail Payments Board, where we bring together representatives from the various service providers, financial institutions, infrastructures, and we discuss issues related to standardization and market integration in this field. We also actively involve market groups, where they discuss all these issues. For that reason, whenever we make a recommendation, when we make partner recommendations concerning the security of Internet payments, we will always take under consideration what has been developed by the market and try not to reinvent the wheel.

Mr. Werkema: I would also comment from a Federal Reserve perspective, that we have Strategies for Improving the U.S. Payments System. I have a leadership role there, as do others in this room. Our objective is to guide and support the industry as it moves forward in a couple of key areas. One is faster. One is security. Many people in this room are involved in our efforts. But the intent is not to duplicate or replicate what is being done in these private sector initiatives, but to complement, support, and maybe be an additive in our benefit there.

Ms. Garner: A quick question for Treasury. We are very supportive of government efforts to move the ball forward quicker on EMV, and particularly EMV and PIN transactions. But you mentioned merchant reterminalization. Even though you are going to have NFC capabilities, are merchants going to be required to turn on that NFC capability on those terminals?

Mr. Mukherjee: No. At the moment there is no arrangement to enable the NFC technology. In the future, that may change. There are conversations with some of the players that I mentioned earlier, but the answer is no.

Mr. Marshall: Just a question for Anjan. One of our concerns is the incidence of identity theft, and one of the best ways of stopping identity theft is to validate Social Security numbers. But weirdly, we are unable to do that in the United States in the Social Security Administration. So, we have to use private solutions that are not comprehensive. It particularly affects

the underserved. In some cases, we are unable to approve people without credit because we are unable to verify the Social Security number. Is there anything that you can do to solve that for us?

Mr. Mukherjee: OK. Let me take that away and come back to you. I had not heard that from you all before, so I do not have an answer. But it is an interesting question.

Mr. Santhana: Question for Anjan. It is very interesting to hear about the EMV initiative, prepaid debit initiative. However, as a government entity, you have to support the lowest common denominator at all times, and that is what we have heard every time we speak to a government agency. So, you are going to be on the payments acceptance side and on the disbursement side supporting checks until the last check transacts through the payments system. And you have to maintain these inefficiencies. So there are going to be complications in terms of cybercriminals focusing on the legacy systems. What is the plan; what is the thought?

Mr. Mukherjee: That is a great point. It is something we are very focused on. As I mentioned in my opening comments, when one is transitioning from a legacy system and upgrading a system, that often exposes vulnerability. I cannot get into the details about that, but I can tell you generally we are focused on it. Our plan is a mix of technological approach or solution to make sure that again we are adhering to our own mantra of optimizing baseline protection and best practices, recognizing we have systems in transition. And then also as we were talking about earlier, a cultural approach as well. It is a combination of those two things. We are aware that we have multiple, sometimes competing systems and we do have to support all methods of payment that run through our system. But the example I was talking about earlier is really more of a tip of the spear thing. That is to help encourage the private sector to move in a certain direction.

Ms. Padmanabhan: To follow up on Vernon Marshall's question, this is also a question for Anjan. For non-credit application, like for typical deposit applications, we still need to collect a Social Security number and verify it against those databases. However, dealing with many of the underbanked and unbanked, as well as individuals who do not want to provide their Social Security number online for understandable security reasons, that is a pretty big obstacle that issuers are facing. Is there any way to interpret the Bank Secrecy Act that does not require banks to collect

Social Security?

Mr. Mukherjee: That is a good question. Like the other Social Security question, it is not something that I have studied, so unfortunately I cannot give you an answer.

Mr. Werkema: Does anyone in the audience have a suggestion there? OK, Kelly, we will turn the floor back to you.

Mr. Dubbert: Please join me in thanking Gordon and the panelists.

Closing Remarks



Esther L. George

I want to thank the program presenters and discussants for the insights they have brought to this most important and timely issue of retail payments security. The conference has highlighted encouraging areas of progress, including technology, information sharing and collaborative efforts among financial institutions, networks, consumers and regulators. It also has served as a reminder that sizeable challenges remain.

The Federal Reserve has a keen interest in promoting the safety and the security of the nation's payments system, given its impact on the broader economy and public trust. As both an operator and an overseer within the payments system, the Federal Reserve is prepared to leverage its central bank roles to bring about critical improvements for payments security.

Although the Federal Reserve is relatively unique among central banks in terms of its retail payments operator role, public authorities around the world have become more active in raising concerns about retail payments security. Some authorities play explicit roles with public mandates, while others rely on leadership to induce voluntary changes in the industry. In the United States, the central bank has chosen to serve as a leader for a collaborative approach, involving a wide range of payments participants as the path toward improving the system.

This is not a new role for the Federal Reserve. Since its founding, the public has looked to the Federal Reserve to provide leadership on advancing the safety, efficiency and accessibility of the nation's payment system. Congress initially designed the Fed to serve as a payments system operator through the regional Reserve Banks and as an overseer of the system through its supervision of financial institutions. These roles give the Fed relevant insights as we work with others to address the security challenges we face today.

For its own part as an operator, the Fed must consider and ensure the security of its own clearing and settlement activities, and this directly influences a large segment of U.S. retail payments. The Fed's financial services business also provides resources to support development of payment standards, including those related to security. And, there are plans underway to work with the Fed's financial services customers to identify demand for enhanced risk-management products that complement the Federal Reserve's suite of wire, automated clearinghouse (ACH) and check service offerings.

As a payments system overseer, the Federal Reserve and other agencies ensure banks protect their systems from unauthorized access to online banking systems and safeguard sensitive personal or account information. In the case of retail payment fraud, consumers have been protected from significant losses by regulations.

These roles have informed the central bank and enhanced its credibility where it plays a less formal but equally important role—that of leader and catalyst for change. The improvements we seek for greater security in the U.S. payments system do not stem from a specific mandate from Congress, but rather from an interest in ensuring stability and confidence in the payments system.

In this role, the Federal Reserve seeks to drive improvement in the payments system through a collaborative approach, which in the past has led to payments innovations that we take for granted today. Routing numbers on paper checks, the development of the ACH, and the implementation of Check 21 are all examples of diverse interests coming together to find a solution to common challenges.

It is in this spirit that we recently established two task forces to take on today's challenges. These groups are comprised of diverse and committed membership, which will ensure a broad range of perspectives are considered as we move forward.

One task force will focus on identifying and evaluating approaches for implementing a safe, ubiquitous and faster payments capability in the United States. The other task force will provide input on security aspects of a faster payments capability, and serve as a forum to advise the Federal Reserve on how to address security matters and to identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System.

An important question is: How will we judge the success of these efforts? Each task force will be asked to identify the criteria by which they will measure success. In the near term, we will look to the Secure Payments Task Force to articulate key priorities. We will also be looking for evidence of commitment from payments system participants to take action on these priorities.

Longer term, we hope to see this collaboration among industry participants continue, resulting in progress on the development and adoption of effective security standards. We would also hope to see robust research and implementation of processes that result in better data and the ability to closely monitor fraud and identify adverse trends, develop more effective responses and track policy initiatives. Success will mean payments modernization in the United States is well on its way, with adoption that reflects the public's strong confidence in new capabilities.

Time will tell whether this collaborative approach can be successful or whether the Fed needs to take a different approach to foster a modern payments system that serves the needs of a dynamic economy.

It was 10 years ago, in 2005, that the Federal Reserve Bank of Kansas City hosted its first payments conference titled, "Interchange Fees in Credit and Debit Card Markets." During the two days of presentations, discussion and debate among leading economists, industry leaders and policymakers, the need for intervention in the credit and debit markets was hotly contested. By 2010, Congress intervened with regulation.

As we conclude this conference on payments security, I sense a greater degree of consensus around the security challenges we face. As the Federal Reserve begins the work of convening and engaging with stakeholders to achieve a faster, more secure and widely available payments system, the pieces of the puzzle lie before us. Putting them together in a way that maintains the public's confidence is both our challenge and our opportunity.

Conference Attendees

Randi Adelstein

Vice President and Senior Counsel
MasterCard Worldwide

Maria Akers

Payments Specialist
Federal Reserve Bank of Kansas City

Kandice Alter

Assistant Vice President
Federal Reserve Bank of Chicago

Lindsay Anderson

Information Systems Administrator
Jones National Bank & Trust Co.

Traci Angel

Correspondent
The Wall Street Journal

Richard A. Babson

Senior Editor
Federal Reserve Bank of Kansas City

Ann-Marie Bartels

Chief Executive Officer
EPCOR

David Beck

Senior Vice President
Federal Reserve Bank of Richmond,
Baltimore Branch

Kara Bemboom

Assistant Vice President
Federal Reserve Bank of Kansas City

Nick Billman

Counsel
Federal Reserve Bank of Kansas City

Susan Black

Executive Office Information Manager
and Assistant Chief of Staff
Federal Reserve Bank of Cleveland

Terri Bradford

Payments Specialist
Federal Reserve Bank of Kansas City

Maarten Bras

Policy Officer
De Nederlandsche Bank

Peter Burns

Senior Payments Adviser
Heartland Payment Systems Inc.

Harold Butler

Managing Director
Citigroup Inc.

John Carlson

Executive Vice President
Financial Services Information Sharing
and Analysis Center

Laura Chadwick

Director of Commerce and
Entrepreneurship
National Restaurant Association

James Chapman

Director, Research
Canadian Payments Association

Julia Cheney

Assistant Director, Payment Cards
Center
Federal Reserve Bank of Philadelphia

Ashwin Clarke

Manager
Reserve Bank of Australia

Jane Cloninger

Director
Edgar, Dunn & Co.

Denise Connor

Senior Vice President
Federal Reserve Bank of Kansas City

Scott Copeland

Chief Operations Officer
BancFirst Corp.

Kristi Coy

Vice President
Federal Reserve Bank of Kansas City

James Cunha

Senior Vice President
Federal Reserve Bank of Boston

Tanya Cvetan

Assistant Vice President
Federal Reserve Bank of Kansas City

Matthew Davies

Payments Outreach Officer
Federal Reserve Bank of Dallas

Thomas Denton

Application Security Manager
Federal Reserve Bank of Cleveland

Corey Dillon

Senior Regional Director
Office of U.S. Sen. Claire McCaskill

Terry Dooley

Executive Vice President
and Chief Information Officer
SHAZAM Network Inc.

James Dornbrook

Reporter
Kansas City Business Journal

Sean Foley

Assistant Vice President
Federal Reserve Bank of Kansas City

Susan Foley

Senior Associate Director
Board of Governors of the Federal
Reserve System

Alan Fosler

Senior Vice President
Union Bank and Trust Co.

Andy Frank

Vice President
Federal Reserve Bank of Kansas City

Thomas Fuhrman

President
Delta Risk LLC

Chris Gilbert

Chief Information Officer
Bankers' Bank of Kansas

Daniel Gonzalez

Vice President
Federal Reserve Bank of Chicago

Jim Graves

Ph.D. Student
Carnegie Mellon University

Eric Grover

Principal
Intrepid Ventures

Joshua Hanson

Research Associate
Federal Reserve Bank of Kansas City

Joni Hopkins

Manager, District Financial Services
Federal Reserve Bank of Kansas City

Mark Horwedel

Chief Executive Officer
Merchant Advisory Group

Cynthia Jenkins

Senior Director and Group Manager
NACHA

Mark Keeling

Chief Operating Officer
The Bankers Bank

Brandon Kelly

Senior Vice President
FirstBank Holding Co.

Andrew Kennedy

Senior Program Manager
BITS, Financial Services Roundtable

Susan Kenney

Senior Vice President
Federal Reserve Bank of Cleveland

Amy Krenzin

Senior Security and Compliance
Program Manager
Fiserv Inc.

Brandon Lloyd

Vice President of Payables
Solutions Manager
UMB Bank, n.a.

Andrew Luca

Partner
PricewaterhouseCoopers LLP

Todd Mackey

Vice President
Federal Reserve Bank of Kansas City

Jesse Maniff

Payments Analyst
Federal Reserve Bank of Kansas City

Brian Mantel

Vice President
Federal Reserve Bank of Chicago

Zach Markiewicz

Payments Specialist
Federal Reserve Bank of Kansas City

Steve Matthews

Reporter
Bloomberg News

Renu Mehra

Vice President
Federal Reserve Bank of Kansas City

Casey Merolla

Senior Manager
First Annapolis Consulting

Dawn Morhaus

Senior Vice President
Federal Reserve Bank of Kansas City

James Narron

Senior Vice President and Cash
Product Manager
Federal Reserve Bank of San Francisco

Bryan Nash

Chief Information Officer
McHenry Savings Bank

Jackie Nugent

Assistant Vice President
Federal Reserve Bank of Kansas City

Barbara Pacheco

Senior Vice President
Federal Reserve Bank of Kansas City

Suchitra Padmanabhan

President
CB Bancshares Corp.

Karen Pennell

Senior Vice President
Federal Reserve Bank of Kansas City

Mark Perkins

Director of Product Management
Fundtech Ltd.

Elizabeth Provenzano

Vice President of Government Relations
National Retail Federation

Suresh Ramamurthi

Chairman
CBW Bank

Thomas Rea

Executive Vice President
U.S. Bank

Aaron Rosenbaum

Financial Services Analyst
Board of Governors of the Federal
Reserve System

Tim Runnalls

Senior Vice President of Operations
Sales Support
Midwest Independent Bank

John Ryan

President and Chief Executive Officer
Conference of State Bank Supervisors

Tom Salisbury

Small Business Liaison
Office of U.S. Sen. Roy Blunt

Prakash Santhana

Director
Deloitte Advisory

Veronica Sellers

General Counsel and
Senior Vice President
Federal Reserve Bank of Kansas City

Duke Sheow

Chief Credit Officer
Green Dot Bank

Mike Skokan

Executive Vice President, Chief
Financial Officer and Treasurer
Hy-Vee Inc.

Pascal Spittler

Business Requirement Architect
IKEA

Brosie Strada

Vice President
Federal Reserve Bank of Kansas City

Gray Taylor

Executive Director
Conexus Corp.

Connie Theien

Vice President
Federal Reserve Bank of Chicago

Mark Tiggas

Senior Vice President
Wells Fargo Bank

Ashley Tufts

Director of Corporate Affairs and
Communications
American Express

Robert Turner

Senior Vice President and Chief
Operating Officer
Federal Reserve Bank of Richmond

Glen Ulrich

Senior Vice President
U.S. Bank

Tamara Vande Velde

First Vice President and Chief
Information Officer
Capitol Federal Savings Bank

Cheryl Venable

Senior Vice President and Retail
Payments Product Manager
Federal Reserve Bank of Atlanta

David Walker

President and Chief Executive Officer
ECCHO

Hannah Walker

Director of Government Relations
Food Marketing Institute

Bruce Welch

Chief Security Officer
Gilbarco Inc.

Julius Weyman

Vice President
Federal Reserve Bank of Atlanta

Catherine Williams

Head of InterBank Operations
and Industry Affairs
Royal Bank of Canada

Michael Williams

Director of Interchange
The Home Depot

Wendy Wishon

Senior Vice President
EPCOR

Ingrid Wong

Counsel
Federal Reserve Bank of Kansas City

Yuemei Zhang

Managing Systems Architect
Wells Fargo Bank

EDITORIAL SUPPORT

Published by the Federal Reserve Bank of Kansas City

RICHARD A. BABSON, Editorial Advisor

BETH NORMAN SCHNEIDER, Layout Designer

The papers in this publication can be obtained in electronic form from the Federal Reserve Bank of Kansas City's website: www.KansasCityFed.org.
