

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

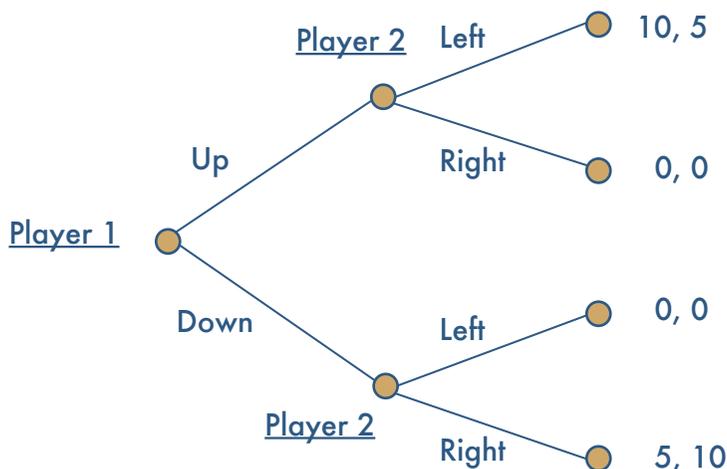
available actions and outcomes represented by a separate payoff for each player. In a game, the outcomes and the actions available to the players are assumed to be common knowledge. In other words, each player knows not only his own payoffs and actions but also the other players' payoffs and actions. 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

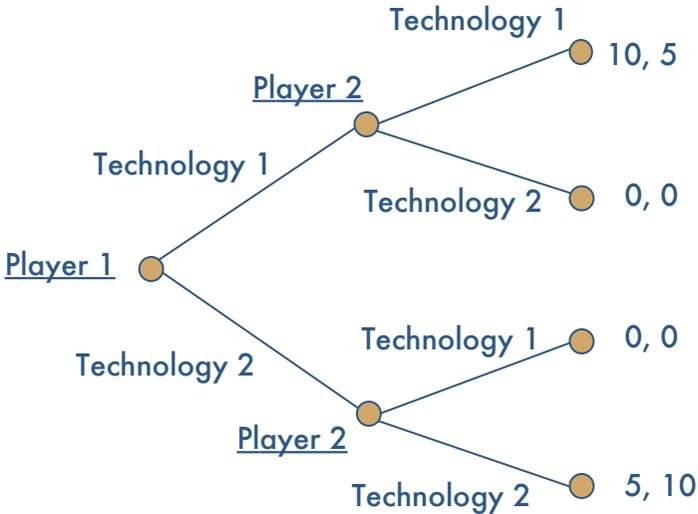
		Player 2	
		Technology 1	Technology 2
Player 1	Technology 1	10, 10	0, 0
	Technology 2	0, 0	10, 10

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? <u>Issuer</u>	
		No	Yes
Adopt EMV? <u>Merchant</u>	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.

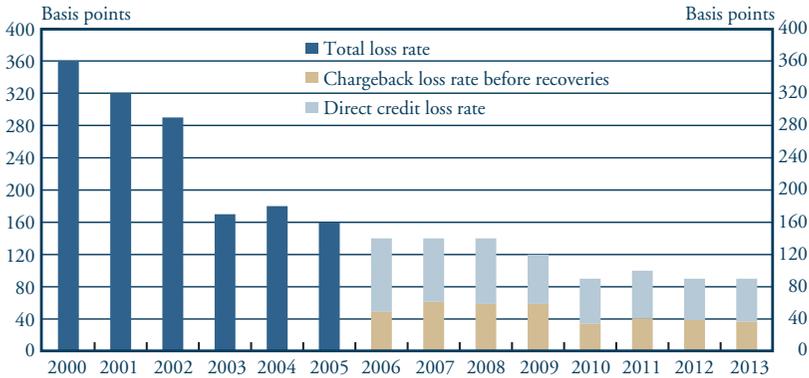
The fourth case study, cryptocurrencies, demonstrates security that is, in some respect, more secure than existing payment methods in that no sensitive account information is transmitted with payments. They may also be the most “disruptive” challenger to existing payment networks. Payment processing 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**

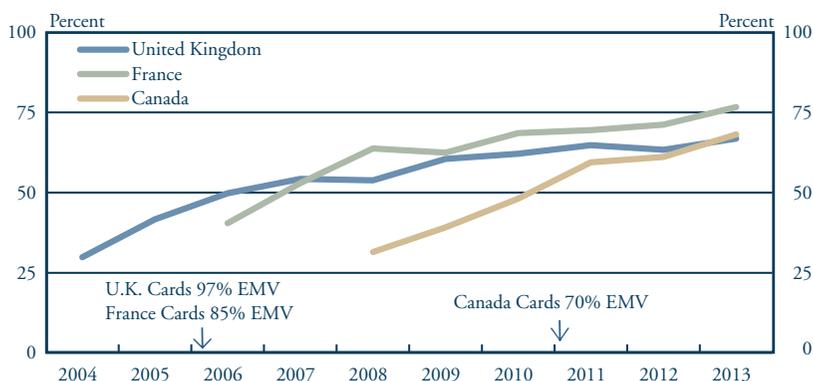
Source: CyberSource (various years).

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

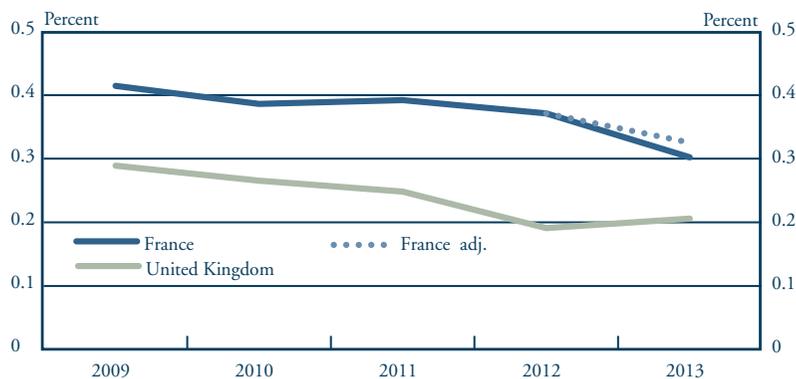
problem (OPCS 2008a). It researched options for securing CNP transactions and cited value of 3DS system in enhanced authentication (OPCS 2008b). It examined consumer attitudes toward security in CNP transactions (OPCS 2009). It engaged card issuers and merchants in a working group and partnered with 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.

