Implications of the Changing Payments Landscape for Integrity of Retail Payments Systems

Moderator: Mark Greene

Mr. Greene: During this panel, we want to discuss some of the stresses on the payments landscape and the fact we have many new payment types—some of which really severed the traditional "Know Your Customer" relationship between banks, merchants, and consumers—such as decoupled debit, which introduced new forms of risk, new opportunities for fraud to take place, new gaps, if you will, in the security continuum we've come to rely on in much of retail payments. That's actually at the heart of what we are going to talk about—the fact that many participants in these new forms of payments often don't have preestablished trust relationships. Therefore, in that world how can you protect against, how can you even detect various forms of attack—fraud, security breaches—that are taking place?

There are a range of issues we worry about, and you'll hear some anecdotal evidence from the panelists about how much fraud is taking place in this evolving world of payments. The short answer is that many of the traditional forms of fraud are well under control, but there is a growing concern about new forms of attack, new forms of fraud.

Figure 1 shows a couple of the tools—the technologies—companies are beginning to deploy. Intelligent profiles is when you take a more comprehensive view of a transaction as it flows across multiple nodes and networks and develop an overall impression of different types of fraud, rather than looking at one particular point, such as a given ATM.

Neural networks, which many of you will be familiar with, are systems that learn over time about new forms of fraud. One of the ways they do that is by incorporating adaptive analytics, which actually detect new patterns of attack, new forms of penetration in much the same way antivirus software can learn, understand and cope with new forms of viruses on your PC.

Figure 1
New Tools for Keeping Retail Payments Safe

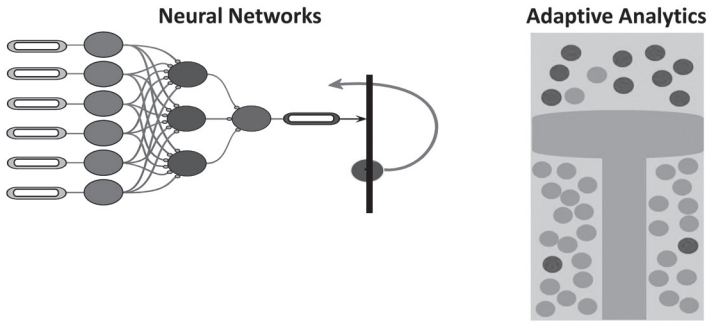


Figure 2 shows that these different types of technologies can be assembled together to provide systemic approaches to some of the risks and attacks we'll be talking about on this panel. I'm not going through this figure here, but suffice it to say, this is a fairly evolving and sophisticated art form.

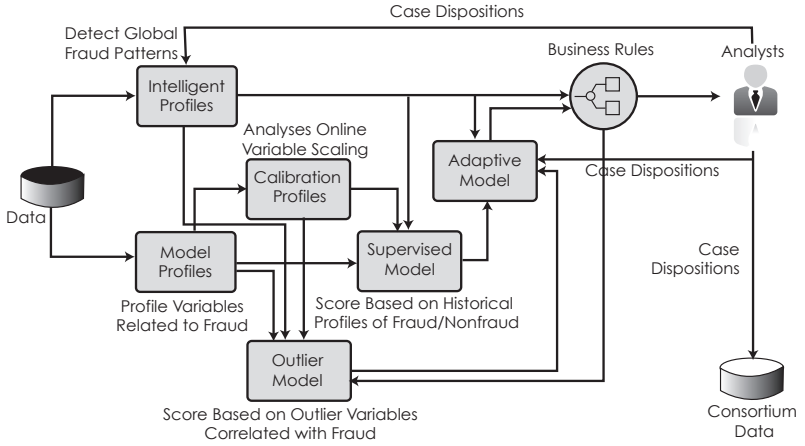
My characterization of the technology approach to these risks these days is that it is a leapfrog game. The bad guys are always looking to push the envelope and find new ways of attacking, and our response as an industry is to try to be equally smart at incorporating new technologies and evolving our approach. This is a snapshot of today's best practice, but certainly the picture will look different tomorrow as the bad guys get even smarter about how to attack some of these systems.

So, with that as a setup, we'll begin the panel with Cathy Allen taking the consumer point of view.

Ms. Allen: Some of us just came from the Atlanta Fed's Forum on Payments Risk that Cliff Stanford and Rich Oliver organized. It was an excellent forum, and I will be bringing some of those insights from the forum into my opening remarks. It was an eye-opening session. There was one panel with representatives from the Department of Justice, the FBI, and the Secret Service, who discussed organized crime and payments risk. We all wanted to go home and cover our heads after we heard about their cases.

My caveat is that I grew up in a banking family here in Missouri. My father, my grandfather, and my great-grandfather were bankers. So I grew up thinking bankers were pretty good people and they did the right thing for the community and for their customers. Unfortunately, I don't always hold that view toward what's happened with financial institutions in more recent times, so I am going to talk a little bit about that. I do believe we're in a transformational time in the financial services industry, and we're going to need transformational leaders and thinking to really get us out of this mess and ready to move the economy forward.

Figure 2
A Systemic Approach to Retail Payments Integrity



The group in this room is an important part of that. You are researchers and thinkers, and we have to take a much more proactive role with our leadership in the financial community to be able to make the kinds of changes that need to happen. I believe we are facing the equivalent of our industry's oil spill, and that means we are in trouble with our customers, with the media, with the legislators. It is something that has been driven by the eroded trust we have—the trust between financial institutions and other institutions, between financial institutions and their customers, and between the public and their regulatory agencies. The media is "on" this issue and will continue to be on this for some time.

The legislators are reacting to consumers. What are we seeing? We are seeing a backlash against regulators, including the Fed. We are seeing anger at banks, at the bank executives, and at the bank employees. We are seeing the growth of internal fraud from disenfranchised and disgruntled employees. We are seeing complaints to legislatures, to the FTC, to the regulators, to the Department of Justice, and to states' attorneys general. We have just begun to see civil suits against financial institutions because of the anger that is there.

Sixty-seven percent of people (this is a recent survey) say they will walk away from their current financial institution as soon as the economy gets better. They are smart enough to understand they have to maintain those current relationships, whether it's a mortgage relationship or a credit card, but they are going to move as soon as the economy gets better.

In a recent study by STRATCOM about how people were impacted by the financial crisis, 89 percent of people in the United States said they were affected, and the sectors and industries that were to blame were: mortgage companies (90 percent), lenders (88 percent), the federal government (86 percent), credit card

companies (81 percent), and insurance companies (56 percent). From there it went down to other kinds of corporations. Truly, the kind of anger that is out there is something we do not want to underestimate.

Fortunately, a recent BAI study of 5,000 executives in the industry actually said that understanding and restoring trust with their customers and improving the image their customers have was important to 50 percent of those executives. I would argue it should be 100 percent, but it is not there yet.

Two major risks we're facing: One is this eroded trust that is one of the emerging risks; I think reputational risk will move right up there along with operational risk as something to watch. And simultaneously we are also seeing greater risks from fraud, cyber-security threats, breaches, and other technology-based threats that serve to also undermine the public's belief in the financial system. All you have to do is talk to businesses about the rash of ACH corporate account takeovers in treasury management and you have a perfect storm of attacking the safety and soundness principles we have.

Unfortunately, I believe our leadership in the financial community has not stepped up. Very little has been done and the public is angry about that. In fact, that old adage, "We're mad and we're not going to take it anymore," is where consumers are. It's not just consumers, it's small businesses, and it's corporate entities. Some examples of why they're mad and why the payments system is in the center of this are:

1) The increased fees and interest rates, and the increased non-sufficient funds fees. In fact, there have been studies to show the equivalent interest rate is 400 percent. It starts to make payday lenders look like reasonable alternatives.

2) The cutting off of lines of credit for small businesses and corporations. And I can tell you war stories about that, where a form letter will come to many of the businesses we have in the United States just saying, You no longer have your line of credit or your loan has been called in.

3) The rudeness of many of the customer service representatives and tellers to the customers that come in to the branches or call customer service.

4) The increased incidences of data breaches, which might cause a consumer to want a new credit card from their issuer every quarter.

Again, these instances reinforce concerns about takeovers and who is really watching out for the consumer. These are examples of what has led to the interest in creating a consumer safety commission or, at least, increased regulation and oversight by existing regulators of consumer protection.

One of the greatest challenges our industry faces is, Where will the revenue come from? If we have tightened credit, where will the revenue come from as the fees go down and there is pressure on profits? As credit tightens, will consumers

move to nontraditional players? In other words, the role of payday lenders or other nonbank institutions providing credit will increase. Will that also increase risk in the system?

Finally, What role will nonbanks, such as telcos, play as we move into new emerging technologies?

I am going to stop there, and I'll come back with questions to talk about the two technologies you really have to watch: mobile banking and social networking, and the roles the players like telcos and nontraditional players (the Googles, the Twitters, the Facebook players) will play increasingly in encouraging and driving consumer behavior in that area.

Mr. Greene: And, for the "mad as hell and not going to take it anymore" consumers, the headline on the front page of today's *New York Times*, "Banks Put Squeeze on Customers Ahead of New Credit Rules," and five column inches of examples of the things you were just talking about.

Next, Jim Van Dyke is going to provide us with a history lesson about credit and the consumer.

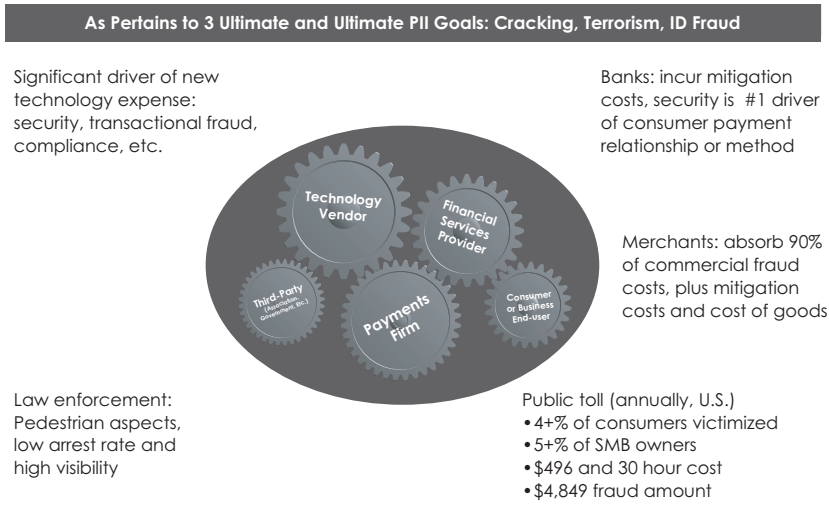
Mr. Van Dyke: I'll start back 110 years ago, and it is quite interesting. To the best of my knowledge, the world's oldest credit card was actually launched right over there, through the window, in Union Station, and it is in our private Javelin collection. I collect old cards, because frankly I find there is such—to put it bluntly—a lack of factual information. You can learn a lot from looking at the history of the payments industry or financial services industry and apply it to how to launch new payment methods.

This particular card was launched by a company that had over 300 horse-drawn buggies out of Union Station. Mallory Duncan, you may want to comment on this and see if the National Retail Federation has a position. There is a public record that shows there was a monopoly charge, an antitrust charge, leveled against this merchant in 1908 after they came out with the first credit card. So here we are discussing payment cards and how that leads to freedom of choice.

Let me move on to Figure 3, which shows payments risk from an ecosystem perspective. We measure banks, consumers, merchants, and processors to try to figure out where there are business opportunities that are currently untapped.

One interesting finding we saw in our most recently released study, which was of 1,000 U.S. multichannel merchants, where we combined loss figures, is a wide disparity between the losses of actual fraud cases here in the United States to the tune of 90 percent that is borne by the merchant, after the consumers pay their $500 of a typically $5,000 crime spree in U.S. dollars. Ninety percent of that remaining cost is paid for by merchants and 10 percent by banks. Given we are talking a lot about interchange and if there is a disparity that needs to be addressed with policy changes, I'm surprised no one is talking about this finding. I have to

Figure 3
Payments Risk from an Ecosystem Perspective



wonder, Could there be an incentives issue that needs to be looked at when that goes on?

We've seen no shortage of consumer motivation. Even when you factor in zero-liability provisions, consumers are motivated; they look at it as their money, their identity. You can give them all the protection in the world and you won't reduce their motivation. We see that in our factual data.

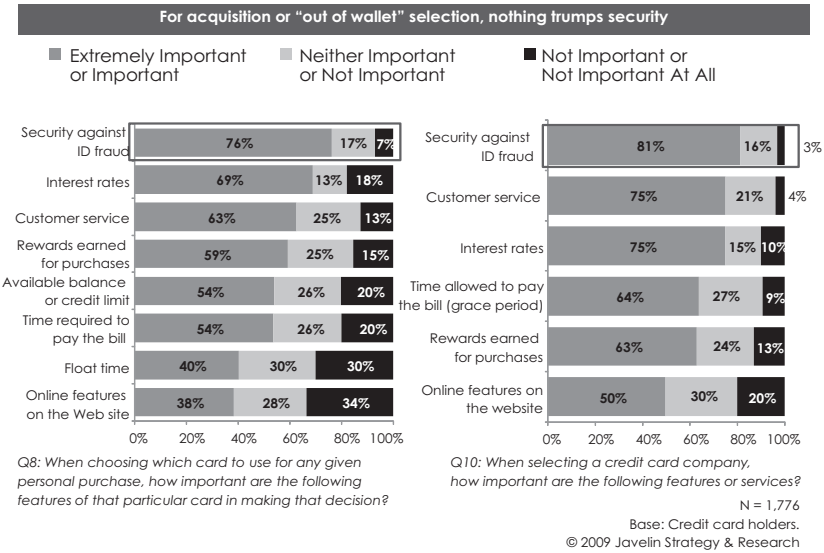
Banks certainly have motivation because of the switching that's going on. And we see switching going up. Consumers are fed up, so that is more of a risk to everybody than ever before. Law enforcement and everybody else bears this cost.

We think there is a way forward, which is what I want to focus on. Chart 1 shows the importance of security in card selection. In our research, we see the risk issue, which is especially high in markets where—like the United States, the UK, and other places around the world—we have worked so hard to achieve frictionless commerce. In some ways, we have achieved frictionless fraud. More bad guys get in as the good people get in.

What we see when we use what is called in the statistical world the aided research method—a series of options are presented to people that basically follows Maslow's hierarchy of needs—is that if you prompt them to think about security, rewards, and many other things, they'll choose security first. Interestingly, a couple of the more prominent marketing successes are based on security.

When American Express Blue, which is no longer positioned around security, was launched one year after PayPal in 1999 before the holiday shopping season it

Chart 1
Security is a Relationship and Marketing Play!
(Remember Blue? Citi's "ID Theft Campaign"?)



was all about security. There was a chip on the card. The system wasn't quite ready to do anything with that chip, but it was launched around security. It was a brilliant marketing move and consumers took to it in droves. People will vote with their feet when they think there is something helping them with security. Citi also had a very prominent identity theft campaign.

Chart 2 shows the relationship between how fast fraud is detected and fraud loss. The faster fraud is detected by the account holder—whether that is a consumer or small/medium business—the lower the value of the fraud loss. So we have a real motivation within the industry to protect people.

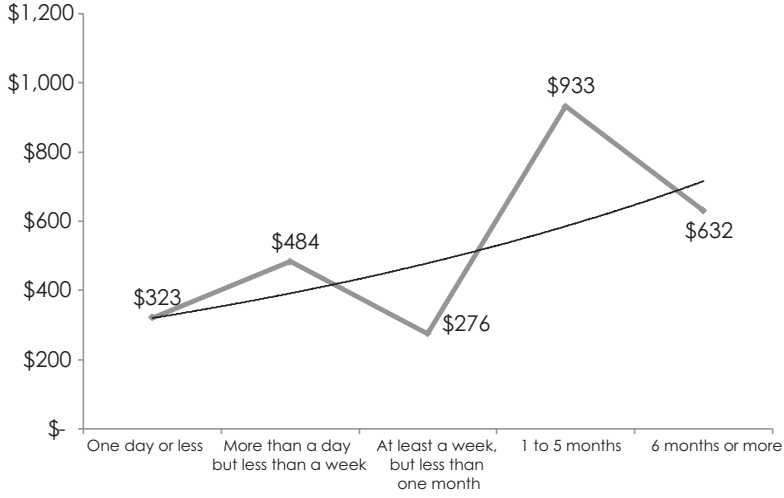
Chart 3 shows fraud victimization rates among data breach victims in the United States. You have a four-in-100 chance of becoming an identity fraud victim. However, if you receive a data breach notification that you threw away and ignored like most people and didn't change your behavior based on it, you have a nearly one-in-five chance of becoming an identity fraud victim. Yet, people lack the education. Even more than education, they lack the tools to make it easy to manage their finances.

Chart 4 shows banks are doing a pretty good job of resolving fraud cases. They are not doing as good a job working cooperatively with their customers at preventing or detecting fraud.

The way forward, as we see it, is to use mobile technologies. Of the technologies that are currently launched, only the music industry allows people to personalize content. The technology is out there. The consumer will is out there.

Chart 2
Disconnect with Notification May Increase Time to Detect Fraud

In crimes of impersonation, victim–empowerment has tangible value

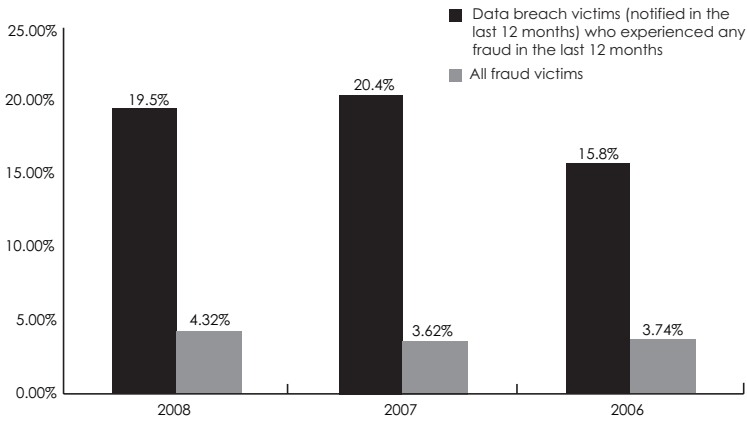


Q25: From the time the misuse of your information first began, how long did it take you to discover it had been misused? by Q34: How much money did you pay out of pocket as a result of the identity theft?

October 2008, n = 475
Base: All fraud victims.

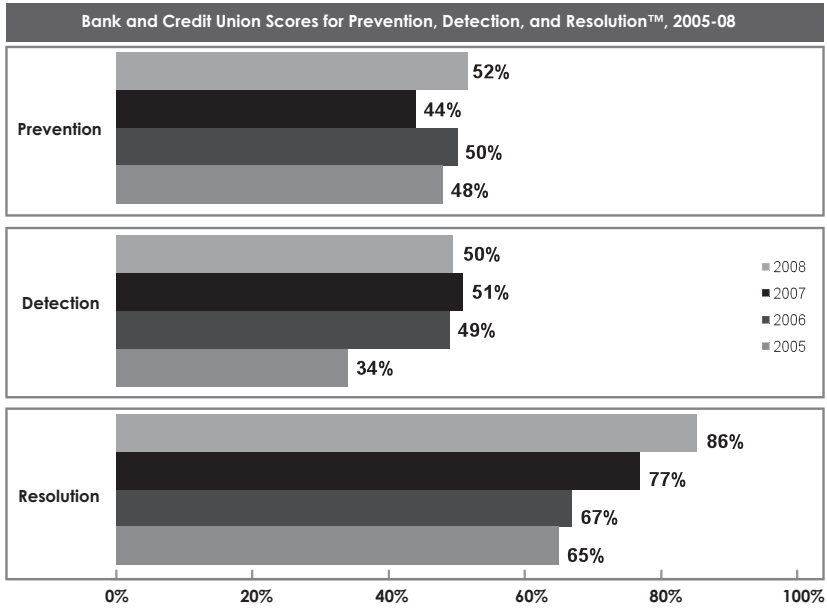
Chart 3
Four Times Higher Fraud Victimization Rate Among Data Breach Victims

Data show that fraud victims rarely attribute transaction fraud to the breach



October 2008, 2007, 2006
n= 539, 535, 552/n= 4874, 5075, 5000
Base: Data breach victims, all U.S. adults.

Chart 4
Many Banks' Best "Customer Control" Capabilities Actually Are About Clean-up



n=25
Base: All FIs surveyed.

We just haven't seen adoption of it in the financial services industry. It is a way to reduce fraud. It is good for business, good for merchants, good for banks, and good for processors. We're just holding back on giving people what they want. And we can reduce the cost of fraud by $50 billion, reduce risk, and make the whole industry more successful.

Mr. Greene: Now we have somebody who actually lives on the other side of this equation and sees the fraud and the attacks from the banking perspective. Daniel Eckert, your perspective please.

Mr. Eckert: I will disclaim a couple things. One, at HSBC I actually run our Business Development, Market Intelligence, Card Scheme Management, and Payment Products Group. So I focus very much on the alternative side of the payments industry and not the core credit card industry. So, if everyone was worried that you could have a tar-and-feather party afterwards of me, I focus actually on the other side in the marketplace in looking at alternative ways to serve both our retail customer clientele, as well as our cardholders.

Second, I just would like to state for the record that the views expressed on this panel are my own, and are not necessarily the views held by HSBC.

I am going to switch gears just a little bit to an issuer's perspective, especially focusing on the innovation front and the alternative payments front on some observations I've seen in spending almost a decade in the alternative payments area. When we look at the payments marketplace from an issuer perspective, with the recent economic recession we're experiencing and the tremendous shock we're seeing as a result of regulatory intervention, as well as credit risk intervention in the credit card markets, I guess it goes without saying that it's a very dynamic time to be an issuer in the marketplace. HSBC in North America is about the fifth-largest issuer of credit and debit cards in the United States and, I think, the third-largest global issuer of credit and debit cards in the world, operating in 43 countries—15 of which we have a million-plus card operations.

Something interesting that is going on—and Mark Zandi among other economists just reported on it—is that as a result of the CARD Act (Regulation AA) and the specter of the Basel II Accord being more pervasive in the global economy, fully $1.3 trillion is going to be sucked out of the credit card system.

Yet the convenience and use of plastic payments still remain. And as a result you have, if you will, a water balloon effect, where if you squish the bottom and it contracts there, the need and demand for that same convenience in alternative payment forms is going to budge out in another area. And it's going to happen quite quickly, much like if you saw a child do a water balloon squishing event.

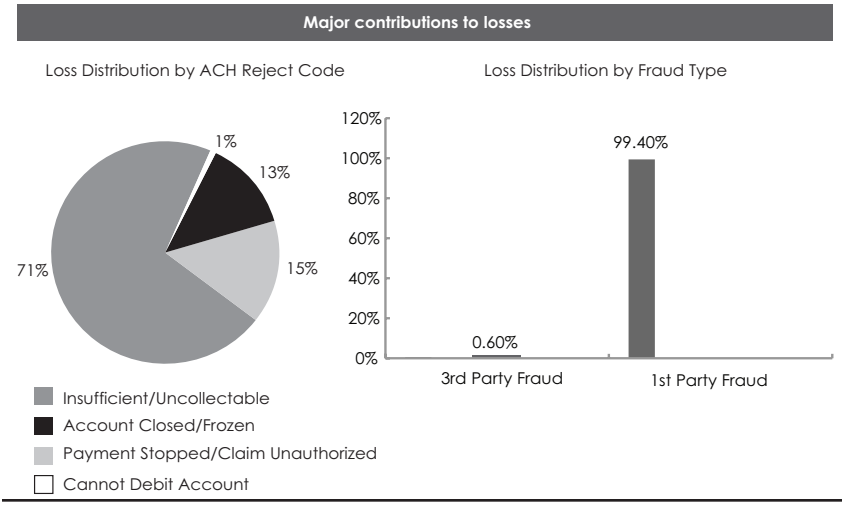
As a result of that, the adaptation that has to occur to ensure the safety and soundness of the system as that scale migrates to a different form of payment needs to be there in order for innovation to thrive and succeed. What is interesting about the legacy payments infrastructure is that far and away you see the innovative set—whether it is the PayPals, the Amazon.coms using ACH debit, or HSBC themselves using their independent debit OptiPay product—leveraging the existing infrastructure to find novel ways to connect the payments plumbing to create value and address consumer needs. However, the challenge is that the plumbing is slow to adapt to those needs. As a result, it very often can stifle innovation.

I want to share—probably for the first time in recent memory—some results of what we have seen, particularly in leveraging independent debit or the ACH network to solve consumer needs and retailer needs. On Chart 5 you will see what we are finding by far and away is that we, and I would say the other sets, are doing a very good job of detecting and preventing any alternative payments structures' third-party fraud—that is, those that are found from account takeover from identity theft or stealing one's account number.

What we are finding, however, is that most of the fraud we're experiencing is of a first-party nature: known identity, validated data using "Know Your Customer" regulatory checks under FACT Act, etc., and yet the person is using the gaps in the current infrastructure to exploit opportunities to just steal—just plain steal—money.

If you look at how they're doing that, as you can see, 0.6 percent of our actual

Chart 5
Infastructure and Rule-set Exploitation is Significant, While 3rd Party Fraud Remains Sparse



losses with independent debit is third party, where 99.4 percent of our actualized losses is true first-party fraud—people kiting e-checks, if you will. How they're doing it is pretty remarkable. They're doing two things. They are exploiting tiny gaps in an antiquated system called the ACH in the United States, where we have to conduct an authorization to pay and we act as check guarantor to pay that authorization, but wait days, potentially up to eight days, to receive notification on whether or not funds have actually cleared. There are customers that notice and take advantage of it, and we end up being out the money when it comes from an issuer perspective.

They are using is very, very strong consumer protections afforded them in the private regulatory bodywork, called the ACH rules. In effect, if customers call up their bank and state the payment for any reason was unauthorized, what occurs in the clearing system is we receive a notification of unauthorized payment—whether or not there is an affidavit that is associated with it really doesn't matter—and we eat that payment.

We have very, very little recourse with the receiving depository financial institution side to even dispute when we actually have a standing authorization to debit. We are seeing about 13 percent of our losses come just from that exploitative gap.

Another thing we are seeing is there are new types of risks that occur when we go into the alternative payments and innovations set within this industry. And that is, How do you validate a customer who may have a disassociated account relationship with you? They may have—whether it's in a digital wallet space, or if it's in an e-check space, or in a web bill payment space or even in a decoupled debit

space—they are establishing a relationship with a service provider but also have an account relationship with an underlying institution.

That poses unique challenges for institutions. One of the things we've seen is a rash of first-party fraud related to perpetrating those types of attacks. It requires money, investment, time, and knowledge to actually suck those out and ensure they get shut down before a rapid loss-making opportunity occurs for the institution.

Table 1 shows an actual mainframe data extract of some of the things we're seeing. This is a first-party fraud, a type of environment where a collective in and around an apartment complex saw an opportunity to take relatively small dollars, but amass many, many dollars at hand, and our systems had to adapt, overcome, and overtake that penetrating event.

You can see our system was learning as it went—final status: "A" being approved and "R" being rejected—through different schemes and trials, but all the same e-mail address coming in on different names.

You can see how our computer system started to adapt with a neural network, address matching, and e-mail address duplication matching to start shutting down the opportunity.

But these things do not come without costs. They do not come without investments in knowledge. And they also do not come without adaptation to the existing infrastructure, too. In order for innovation to succeed, that adaptation has to occur. Otherwise, innovation can be stunted.

Mr. Greene: Paola Masi will provide the central bank point of view. In Italy in particular, a lot of these payments processes are outsourced, so there are the additional risks to the system of things outside the conventional central bank oversight.

Ms. Masi: Thank you for inviting me to present the first results of Banca d'Italia's survey on the role and risks involved in the outsourcing of electronic retail payments to technical service providers. The latter are very often nonbanking-owned companies. We started our investigations on the stimulus of the findings of the Federal Reserve Bank of Kansas City and the ECB research on nonbanks in the payments system. In particular, we tried to answer some questions raised by Stuart Weiner and Simonetta Rosati's paper on this topic (Weiner, Rosati, et al., 2007); that is, to understand how nonbanks are affecting the global payments system risk profile.

After a fruitful seminar with Stuart in Rome, and the involvement of our colleagues from banking supervision, we defined the methodology and the contents of the project. The idea was to define a questionnaire to be filled in by banks in order to build a database of technical service providers for oversight purposes and to measure the perceptions of risks related to outsourcing in retail payments. For each payment cycle, we identified 15 main activities and five main phases (pre-transaction, transaction, clearing and settlement, post-transaction). Then we asked banks to score and name their outsourcers for any of these activities.

Table 1
Anatomy of 1st Party Fraud Ring

EMAIL_ ADDRESS	APPLICANT_NAME	FINAL STATUS	STREET ADDRESS
JAQUEZXXX@YYYYYYY.COM	J. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J.D. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. D. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. D. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J.D. MITCHELL	R	607 BAYWOOD COURT
PEXXXX@YYYYYYYY.NET	P. OWENS	A	607 BAYWOOD COURT #607
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWENS	A	607 BAYWOOD COURT #607
NMXXXXX@YYY.COM	P. MARTINEZ	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. MARTINEZ	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	R. MARTINEZ	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	R. MARTINEZ	A	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	R. MARTINEZ	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	J. FUDGE JR.	A	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	J. FUDGE JR	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	M. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	M. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. MARTINEZ	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. MARTINEZ	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. FUDGE	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. FUDGE JR	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. FUDGE JR	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	Q.D. MITCHELL	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	Q MITCHELL	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	C. GRANT	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	J. STARKS	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. MARTINEZ	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	W. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	W. MITCHELL	A	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. OWES	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	D. STARKS	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	D. STARKS	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	M. L. JOHNSON	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	M. JOHNSON	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	M. L. JOHNSON	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	M.E. JOHNSON	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXXX@YYYYYYY.NET	R. MARTINEZ	R	6726 TARA BLVD #19B
JAQUEZXXXXXXXX@YYYYYYY.NET	P.A. OWENS	R	607 BAYWOOD COURT

Table 1 (continued)

JAQUEZXXXXXXX@YYYYYYY.NET	P.A. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	M. JOHNSON	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	M. L. JOHNSON	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	J.D. MITCHELL	R	607 BAYWOOD COURT #607
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWNES	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	J. STARKS	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	J. FUDGE JR	R	607 BAYWOOD COURT
JAQUEZXXXXXXX@YYYYYYY.NET	P. OWENS	R	607 BAYWOOD COURT

The survey questionnaire can be found on the Banca d'Italia website, in the "Oversight" section.

The survey involved all Italian banks, and the answers covered almost 85 percent of the retail payments industry in Italy. According to our findings, on average, each bank uses three outsourcers for each card payment and two for each credit transfer/direct debit; these outsourcers might be bank-owned or nonbank-owned. The market structure of technical service providers for payment services in Italy shows a huge number of companies: Banks named more than 170. However, only the first 10 providers are important in the system (they account for more than 75 percent of the answers). It turns out that we have a very competitive market, with a great number of suppliers, and the prevalence of a few technical service providers to which all the activities are outsourced. This might indicate that the potential for mergers and acquisitions in Italy is still high.

There is still a lot to understand from the ownership structure of these technical service providers. According to the survey, only 55 percent of them are bank-owned companies while the remaining 45 percent are nonbanks. But do banks fear the outsourcing to nonbanks more than that to the bank-owned ones? Well, surprisingly, the data give a negative answer. There is not such a huge difference in the perception of risks that can be directly linked to the ownership structure: What seems to be important (and eventually scary) for a bank is the outsourcing "per se," not the ownership structure of the outsourcer. Among the first 10 outsourcers in Italy, there are a few big international companies, which are operating worldwide. From the point of view of banking risks, and also for regulators, this seems to be an interesting point: Information, strategies, data, controls and legal frameworks might be more difficult to govern with only a national perspective.

Based on their past experience, banks scored the perceived risks in outsourcing. According to the results, they are rating fraud as one of the most serious risk events; the most frequent losses are observed in the case of operational

disruptions and frauds; the highest impact in economic terms is on "reputation" and on bank reliability towards costumers; the most critical phase, which is commonly outsourced in the handling of a payment cycle, is the "transaction phase"—which according to our definition, includes relevant activities such as the identification of the customer, the verification of credit lines, fraud screening devices, checking of eventual black lists, etc.

As for perceived threats, based on bank expectations and not on effectual losses, most concerns are related to possible malfunctionings in the use of devices (e.g., POS), including Internet access to payment instruments. Again, as you might foresee, the most feared events are fraud and Internet attacks.

Up to now, given that the analysis is still ongoing, it is possible to highlight four main aspects. First, card payments—in all phases—are outsourced more than credit transfers/direct debits, and this is to be considered in the analysis of the card payments industry. Second, the market structure of the technical service providers is an interesting part of the story to be better understood, above all, in monitoring the consolidation process. Third, I think we should evaluate the implications for market players and regulators of the international dimension of some technical service providers, since they provide not only retail but also large value payments and services. Fourth, there is also a global dimension for some phenomena like fraud, which strongly deserve further attention by overseers and by the market in order to progress in international cooperation.

Mr. Greene: Some of you will remember the old U.S. television show, "Hill Street Blues," where the sergeant says, "Hey, be careful out there!"

That's the spirit of this panel. There are bad things that happen out there. So to better understand that and to crawl into some of these remarks, Jim, could I ask you, Are fraud and loss getting worse or not in retail payments?

What does the data show in terms of actual number of attacks and dollars of attacks?

Mr. Van Dyke: Data show quite clearly it is getting worse.

Mr. Greene: So, if it's not a notional topic that we have, it's a real-world phenomenon. Then the nature of that, which is both some of the threat and the opportunity—Cathy, you were talking about two technologies in particular: social networking and mobile. Maybe you could expound on why you think those are the relevant places to look.

Ms. Allen: Right, and it really is scary out there, because emerging technologies can lead to an erosion of trust. We're dealing with something we have never dealt with before and that is organized criminals who use the Internet.

They have web forums. They are as organized as business entities or military organizations. Sometimes they've never met each other, other than through the Internet. And they play different roles, from sniffers to card dumpers. There is a

carding forum where, if a criminal has done a breach and wants to know what to do with the names (like where to sell them), they can find help. And there are actually money-back guarantees if the names don't garner money.

Something like 40 percent of the breaches take anywhere from 10 to 100,000 names. Often the hackers sit on the names and account numbers for awhile. The programs we have right now, for instance, for six months or a year of credit watch, really aren't effective when you look at how sophisticated the criminals are. Many of them are bank employees. In 32 to 40 percent of the cases (this came through some of the comments that were made last week by law enforcement, as well as Verizon's security business that does this) there is some kind of partner inside the organization, someone who knows the financial system or facilitates a Trojan being put onto a corporate treasury computer, or who at least knows how to work the system.

So we're not dealing with mom-and-pop criminals. We're not dealing with localized groups. We're dealing with organized crime. If you see how the FBI analyzes cases, you see there are links between criminals in Mexico, Asia, the United States, and the Ukraine. There are people working all the time through the Internet to commit crime.

Mobile banking is going to escalate fraud. Again, we don't have the appropriate security measures in place. Over 98 percent of the people in the United States will have cell phones by 2011. Of course, abroad it has been much more prevalent.

The latest trend in terms of cyber thieves is to go after Facebook, LinkedIn, and MySpace to use it to compile information on consumers to obtain information to take over accounts. Again, as we see those entities, whether it is through mobile banking or through peer-to-peer loans and payments that are done through the social networking sites, you are going to see the criminals taking a much stronger approach.

Mr. Greene: Two thoughts there: You're right about the mobile thing. I bank at a top-five bank and they have very robust security when I go to the regular website from my PC, but when I'm on my cell phone it is a simple password that's used and it's much easier to get in and do mischief on the cell phone than it would be on other channels.

The one good thing about social networking is it is not just the bad guys who are using it. It is increasingly being used by people inside the industry to self-police and spot problems.

There is a website some of you are already familiar with that might be worth checking out in this regard. It is called *fraudalertnetwork.com. Fraudalertnetwork.com* has several thousand professionals from the banking industry who are regularly reporting new forms of fraud and defenses against them. It is a very good information exchange regarding this problem.

Ms. Allen: There are two statistics that I think are important for all of us to keep in mind: First of all, there are 77 million GenYers, just the same number as

baby boomers. It is the GenYers who are going to use mobile banking. They are going to drive what happens there. So we have a huge part of the population who will *only* use or want to use some kind of a mobile device.

The other thing is that Facebook alone has 300 million users, and 120 million of them log in every day. It starts to shift this relationship of who owns that customer, who has the interface with the customer. I think we'll come back to talk about this, but really watch the new roles for telcos, for the Facebooks, the Googles, who have the customer relationship. Now they are adding payments or payments-like transactions.

Mr. Greene: Dan, those are your customers we're talking about. And now they are Facebook customers instead is what Cathy is saying.

Mr. Eckert: Well, the banking industry is going through a dynamic change in terms of customer relationship and how customers are viewing that relationship, to tell you the truth. Matthew Bennett had mentioned, and I cite the study often as well, about the grist mill in terms of current account relationships. McKinsey did a study about the United States and I think it reported that only about 3 percent of the U.S. DDA population changes hands in any given year. The reasons behind that 3 percent grist mill, and it's an absolute fact just like Matthew had mentioned, are divorce—you're more willing to change your long-term partner quicker than you are to move your bank; death is the next one, because you have to settle accounts for estates; and finally choice. Yes, it's a sticky relationship, but the nature by which they're accessing that relationship is changing, and the way in which they view that relationship is much more from "That's where I place my funds, but where do I gain that satisfying experience, and where do I feel as if I'm getting a great relationship?"

And it very well may be at Facebook. It may be, as you're seeing in the innovation center in cards, the decoupling nature of that, where a retailer can issue. Shell Saver Card is a great private-label example, where a card can be issued by a brand that has a stronger affinity than that of the underlying current account source. It's certainly happening and it's happening in many ways. As that volume comes without careful attention as to how to structure those, it clearly will create opportunities and avenues for frequent and highly severe losses to be incurred.

Mr. Greene: One way of both strengthening the relationships and also getting ahead on some of the criminal activity Cathy was talking about is by understanding how consumers want to think about their own personally identifiable information (PII) and how they want banks to handle that.

Jim, I know you spent a lot of time looking at that. Talk about the role of PII as the interface between consumers and banks in this discussion.

Mr. Van Dyke: There is this commonly held view within the payments industry, as well as the credit-monitoring industry, that people aren't motivated to protect themselves. I will tell you just flatly we see the exact opposite in our data.

As I said earlier, there is this popular misconception zero liability somehow lessens people's motivation to act. We've never seen a shred of evidence to support that. We only see evidence to the contrary. The more you give people good controls, the more motivated they become. Now it is better to not just resolve the fraud after the fact, but actually put the tools in their hands.

One of the problems we have in the industry today is we take the payments industry plus the regulatory stance: By proposing new ways of encouraging positive action to make bad things happen only to criminals, we encourage a very "paternalistic" stance. That is, we try to be like the parent and treat the customer like a child.

Of course, it's good to have great technologies that we would be lost without. These are vital technologies, like geolocation, neural nets, fraud filters, and all these important things, and sharing of data behind the scenes and so forth. We have to have those. The thing is we somehow spread these misconceptions that people aren't motivated to protect themselves. Our data show that for consumers, all other things being equal, security is not only the number 1 criterion when choosing a new institution, it's also the number 1 criterion when choosing which card to use out of wallet. That has never *not* been the case.

When people don't act like we showed in our data breach study, it's because they're confused and they get these very onerous tools and sets of information that are very confusing. One quick example for those people who use electronic music services: If you were to sign up for a song—those of you who use e-music and have an iPod or use Pandora and hear a song you don't like and you never want to hear that one again—if you use electronic music, it's very easy. You click the button, "Don't Play That Again." Those who use that, you know what that is like and know what I'm talking about.

Could you imagine if you were listening to electronic music, a song comes on you don't like it, and you hear it on your iPod and it says, "Well, to not hear that again, go to your desktop (which is maybe at home), login, authenticate yourself, go to a control panel, click on some radio buttons. Oh, that's not under the card section, that's under the DDA section." The point being that is what the banking industry does. We have tremendous opportunity.

Mr. Greene: This may set up the question I was going to ask Dan, but any of the rest of the panel can respond.

One way of thinking about the kinds of problems we're seeing—both the consumer frustration and the new forms of attack—is really trying to run newfangled payment products on what you, Dan, called "on old-fashioned rails"—ride on the back of things like ACH and so on that were never really designed for that.

I was struck by the fact, in the retail payments space, the need for a new generation network that might have the low cost that's needed, the security, the reliability, those are problems the wholesale payments space faced years ago, and their answer there was networks like SWIFT. We don't seem to have a similar

evolution here. What's the view from a banking perspective? Would you like to see movement toward a new-generation network? Or are you comfortable riding old rails?

Mr. Eckert: It's a great comment. At HSBC, I was fortunate enough to actually be part of an attempt to develop an alternative payment network that was merchant-centric. We actually hold an investment in Tempo Payments, which was exclusively designed to be a merchant-friendly network whose aim was to lower the cost of interchange to something that is highly manageable, and to build acceptance on a secure type of rail that is PIN only. It's interesting to point out that customers—on average—tend to prefer PIN authenticated payments, and it's also a more secure form of payment in the retail payments ecosystem than, say, for signature. The move away from signature-based payments and toward PIN—or even better—chip and PIN authentication would likely advantage all participants in the payments market. Add to that a network whose sole aim was designed around making merchant payment acceptance a low-cost proposition, and you'd think you'd have a slam dunk of an opportunity in payments. But, before going into my thoughts on why it became such a challenge to be successful with that model, allow me to say a few words on the chip and PIN card model.

As a recent analog, the UK just recently mandated to go to chip and PIN as a region. The results from the first half of 2009 show that bank card fraud is down 23 percent. What's even more interesting and intriguing is the report stated that second-order effects are also occurring, where in the UK you can still do "card-not-present" transactions without the chip and PIN because that is the only way you can do it. However, even with this "less than perfect" construct, bank card fraud on card-not-present transactions is down by 18 percent.

There's clearly an ability to do something like this in the United States. The challenge, though, and I've experienced it first hand, is the retail payments landscape is an extraordinarily robust and deep marketplace here within the United States that required billions and billions in investment from its participants to build and maintain a network. For most of its history, this investment was made under the so-called association model. And that cost was borne by the member banks in order to actually promote acceptance, to invest in those acceptance marks, and to afford convenience to retailers providing that acceptance network. However, only now in the last 20 or so years really have those economic rents started to mature to a return. And we are now obviously having a debate as to how much of a return that is.

What we fail to understand is in 1953 when those types of networks started, a humongous amount of money and a tremendous amount of capital inefficiency went into building that type of network. And, when faced with an alternative—such as Tempo Payments—the ability to actually invest in that capital-inefficient model for a 50-year return on investment is just not there. It is not there in the investment markets. It is not there in the venture markets. And, even for an institution

such as HSBC who can invest in a capital-inefficient kind of investment, we found it a true struggle to move beyond acceptance in the United States to about 700,000 participating locations. Beyond 700,000 participating locations, you were looking at a door-to-door investment effort to try to get acceptance.

Another great empirical model to take a look at is Discover Financial Services that continues to build—and has been successful in building—a fair bit of acceptance as a three-party system, but still is nowhere near that of our ubiquitous networks such as MasterCard and Visa. So it is a real challenge to do. That is why you're very much seeing innovation flourish within the existing plumbing, so to speak. At the end of the day, it's easier to build on something that's already been invested in and works and operates, as opposed to trying to compete against that broad and deep marketplace.

Mr. Greene: Okay, but if we're worrying about integrity with new payment instruments, we'll have to do so within the context of existing infrastructures.

Mr. Eckert: I think you're exactly right and it's because, when you look at the model, if you talk to any venture capitalists—especially today and in the last year and a half—the only buzz-worthy investments they are making are: "It has to be capital-efficient and I need to be able to put as few dollars into the equation and get the maximum amount of dollars out of the equation." If you were to walk into a VC today—Sequoia or anyone of those—and say, "Hey, I've got a great idea. If you give me $3 billion, I could probably get you a million participating merchants," they'd kick you out of the office.

The infrastructure just isn't there to invest in it.

Ms. Masi: Just a question. Our survey tells us that banks outsource at least 40 percent of the activities of any payment chain. From a bank perspective, the more the outsourcing activity is standardized, the more the internal controls are easy and automatic.

As a result my point is: If a payment is a "commodity," where everything is standardized and easy to control, we do not need to pay great attention; the true problem is innovation, and we should focus our attention and worries only on new payments, with no clear standard.

Mr. Eckert: I guess I could respond in saying we are probably the wrong institution to ask, because we actually own about 95 percent of our systems. We are one of the rarities in global banking, where we own, operate, and enhance our systems—and view it as a competitive advantage.

It's publicly available data that we are endeavoring on a global technology initiative to bring to the 21st century our owned and operated technology systems, because we view it as a sustainable, competitive advantage in the marketplace.

Mr. Greene: You make the regulators sleep well at night when you say that.

Mr. Eckert: I think we do. There are certain systems we still do offer through TPS.

Mr. Greene: I wanted to ask one more question before we throw it open to the audience. It is the one you prompted, Cathy, with your remarks about the need to rekindle trust between consumers and the banks. Do you have some thoughts on how you do that? The bankers in the room should do what to get the consumer to feel better about them, both in payments and more generally in retail banking?

Ms. Allen: The first thing is to apologize to your customers. I oftentimes do that when I'm out speaking in front of consumer groups. Say, "We're sorry. We got you into this mess and we will get you out."

I'm very straight about that, because when the history books are written about what happened with this current economic crisis, a lot of it is going to fall on the shoulders of the financial institutions for a variety of reasons we can talk about.

So, one is to acknowledge that with the consumers, because at least it will dissipate some of the anger.

Second is to treat your customers with respect. I think Jim had some very good points about this. They're not stupid. They get what's going on. To try to hide things, such as fee increases or interest rate increases, to not be transparent is *not* a good thing to do. So being transparent is important.

Third is to help and work with customers to not incur fees. This is where mobile is an important part, where you can send an alert through e-mail or Twitter or texting to say, "Your account is low. You might want either not to take money out of an ATM or not spend, especially with a debit card." So having those kinds of alerts.

Fourth is to enhance financial literacy. There's a lot of controversy about what really works in terms of education, but what we do know does work is education around the transaction. So that if they are getting a mortgage, if they're opening a credit card, if they're getting their debit card, having mandatory education and a way to work with them. Again, Jim's point of being a partner with the customer around security and identity theft—preventive types of issues.

Finally, there is a huge opportunity for the bank that "gets it." There are very few right now that are getting it. This is not a promotion for JPMorgan, but at least what they're saying in their website and in their annual report is a lot more consumer-friendly than most financial institutions are doing. Taking that role as the trusted adviser, helping to simplify the complexity of the financial responsibilities we have, and going back to try to work with the customer.

Again, one of the most egregious things banks did was call in loans and cut off lines of credit, not just for consumers, but for businesses, with form letters. What would it have taken to have an account rep call them up and explain, "We're in an economic downturn. Can we work with you and maybe lower the line of credit?" But, because they didn't do that, we've got a long way to go to restore the trust.

I will end by saying one thing. Trust equates with regulation to the consumer. There are a number of studies that show that. So the more we are going against regulation, the more consumers are going to be skeptical. So the more financial institutions are fighting against increased regulations, the more consumers will be skeptical. I encourage financial institutions to both be proactive and create smart legislation and smart regulation, because that's one of the things that will create trust. Consumers believe the regulators should be looking out for their good.

Mr. Greene: So maybe a jump-off question before we go to the audience. The Consumer Financial Protection Agency that's being debated: Good idea, bad idea, should the banking industry rally behind it or try to self-police, to brand it? Jim.

Mr. Van Dyke: My thought on it is I'm just waiting for any agency—new agency or existing agency—to work for empowering the consumer and the small-medium business customer. If it takes a new one to do that, I'm all for it. But, if that new agency is not going to do that, then I'd just as soon see that same effort go in the existing one. I see a huge void in the existing financial regulatory market today and the commercial market. I'd like to see somebody step up and fill it.

General Discussion
Session 5

Mr. Greene: So, the theme of the panel is about integrity, which seems to have two threads from these remarks. There is a trust thread. Integrity speaks to the belief of all the participants that good things are happening with known counterparties. But, then, there is also a subtext as far as security threats and technical challenges and penetration in attacks, which of course are amplified in an environment where trust is lacking upfront.

Comments and questions from the audience on any of those?

Mr. Grover: I have a comment and a question for Daniel Eckert. You touched on the difficulty of building critical mass in new payments systems and referenced specifically Discover. Discover is on a path to achieving acceptance parity with Visa and MasterCard, at least in the United States, by in effect emulating their open model and by harnessing existing delivery infrastructure through merchant acquirers. At least on a national level, it is difficult but achievable.

You also touched on Debitman. The original Debitman business model was predicated upon retailers originating new cardholders. Any thoughts on why retailers weren't more successful, didn't more vigorously originate Debitman cardholders?

Mr. Eckert: I would say, as reference to Discover, you're absolutely right. They are in many ways emulating the four-party system by working through merchant processors now to gain broader acceptance. It would be interesting—and I have not done this research; if anyone has I'd love to hear a comment on it—to see what the cumulative paid-in capital is into Discover card since its inception and how much it has cost them to achieve the acceptance marks they've had.

The most recent empirical data point is what they paid for a deteriorating network acceptance model, but still, nonetheless, $160 million for Diners Club to at least get some overseas acceptance. If you look at DFS, which was really a domestic

acceptance model with very limited ability to do anything overseas, Diners Club offers them an opportunity to do so at $160 million price tag. I don't know of many new venture capitalists that are willing to plunk down $160 million on a new network. You do have a challenge in terms of how much investment it requires.

As it relates to the Tempo Payments model, you are absolutely right. It was conceived with the purest of intentions and that was one of the reasons why we were so attracted as HSBC to the model—it seemed to have provided the answer to the merchant model. It's PIN-friendly. It seemed like customers prefer PIN, although there is refuted evidence now that says it's a toss-up. It was a low-priced model, a fixed fee for payment; it seemed to have all the characteristics that made sense for merchants' acceptance.

The challenge was two-fold and a bit nuanced. The first challenge is you are dealing with a two-sided market. In hundreds of meetings I've had with retailers about acceptance, the challenge is, "That's great. You're offering me a low-cost model. But, for four cardholders, that doesn't help."

That's just a fact. That was exactly what was said behind closed doors.

The second challenge is then working on the acceptance model through an emulated structure, such as going through merchant processors. It's nuanced because you can sign a deal—let's say with First Data—to gain a great press release that says you have access now to 400,000 accepting retail locations. But that is actually a misnomer.

What that means is you have "technical" access to those accepting locations. You still need to talk to one merchant at a time for them to turn on that access and put up the acceptance marks so that customers are aware the network is accepted. That is a monumental challenge. It is a $1 billion-plus brand-building exercise. It only happens with sneakers on the street, knocking on doors at the local bodega. Yes, you can get some big chunks down with the IKEAs, the Walmarts, the Targets, the Home Depots, the Best Buys, and the Costcos, which is exactly what Revolution Money has been doing and what Tempo had tried to do and finally threw in the towel. By the time you get to, say, 200,000 locations, which sounds like a large number relative to the 4.5 million locations you really need to have somewhat ubiquity in the United States, the amount of money that was required to do so was not able to be raised within the venture capital community.

Ms. Garner: One thing we hear in Washington is banks—and in particular small banks—rely on interchange fee revenues to help cover fraud costs. One example is the reissuance of cards in the event of a data breach, which I would argue is a very reactive type of response.

So, my first question is basically for Catherine Allen and James Van Dyke. Do interchange fee revenues stifle bank incentives to proactively innovate to best protect their customers' data from fraud?

Second, given numbers from James' presentation that merchants absorb 90 percent of commercial fraud costs, etc., does that further disincentivize banks and networks from innovating and implementing stronger fraud prevention technologies proactively?

Mr. Van Dyke: Both merchants and banks do incur significant mitigation costs for all the technologies upfront and all of the customer handling costs of managing costs, so on that front, they're fairly equal. But I do think from an economic analysis standpoint, there are some incentives issues, significant questions raised, when the interchange system allows the bank to keep the profit but pass on a lot of losses to merchants. That is a concern, particularly with the increased amount of data breaches going on. If that cost is largely landing in merchants' laps, that does bring about a motivational question.

Ms. Allen: One of the issues is fraud is increasing. We have sophisticated criminals going after the system, and we have a mandate in the United States to make our customers whole. Somewhere, somebody is going to have to pay for that—the financial institutions. So interchange is one of the places they look to have some revenue coming in as other revenues are moving down. It's unfortunate. As I was talking about the perfect storm, we're hearing banks are increasing fees at all different levels because the revenue streams have gone down in the mortgage area, they've gone down in the basis points in a number of their interest products.

At the same time, the costs of fraud and cyber-security threats are increasing. Unfortunately, right now, financial institutions are even decreasing the amounts of money they are spending on fraud and cyber-security. It's a disaster waiting to happen.

Mr. Greene: As things are going, we take it as a given the consumer will be made whole. The subtitle of this conference is "The Role of the Central Bank." Is there a role for the Fed or other central banks to play in the allocation of loss between banks and merchants—because it's the 90-10 you pointed out, right?

Mr. Burns: I'm fascinated by this whole discussion. Jim, you talk about the possibility of some imbalance in incentives. And Cathy argued interchange is needed to pay for that side of the balance. If you think about these costs, and I'll take your point and I'd like to hear more about it if you do truly believe there may be some imbalance in terms of the allocation of costs. I think, Mark, that is what you're getting at.

How do you create the balance? And I've been thinking for some time that one of the economic tools is to use an interchange vehicle, which from its inception was designed to create a better balance between costs or whatever you might want to call it in terms of acceptance and the original motivation. But can't that tool be extended or can't that conflict be extended to improve or to provide appropriate incentives for other parties within the payments system to invest in fraud protection?

Mr. Van Dyke: Your question is, Should there be more incentives for any other entities to create more effective fraud mitigation capabilities? To me, those are the two issues I see when I look at research on all the entities and the two crimes that are always there of "steal the data, use the data." The most effective way to profit from PII exploits is to go directly into an institution yourself as a bad guy and ride on somebody else's good reputation. That's the most profitable way to do it.

The two issues that stand out in my mind are 1) that you have the person whose identity is being used, no one is empowering them, and people say things that aren't true, like the person is not motivated, they can't make a difference or they will just bother our security experts. Behind the scenes, things have to be there. I'm not saying those aren't important. There's that and then 2) there is this funding equation. I would agree with what you're suggesting, which is that some kind of funding stream needs to go at fixing this problem—which is to take the identity holder and get more tools in their hands. Cathy's point: There are peer-to-peer tools, social and networking tools, and especially mobile tools. I think mobile banking has the safety advantage and is the greatest monitoring device that's with you all the time. But, if the information is not real time and it is not easily modifiable, it's not going to work.

Mr. Greene: There are maybe two thoughts there. There is the incentive to better equip the consumer, but also the 90-10 ratio suggests there is some pricing incentive to move more of the pain toward the banks and away from retailers.

Do you want to defend yourself, Daniel?

Mr. Eckert: Like I said, there will be a tar-and-feathering afterwards. This is the first I've heard of this 90-10 statistic. It seems pretty dramatic. If I look to the marketplace and understand empirically how things could change, one would imagine if 90 percent of the fraud loss occurring in the retail payments system is actually being borne by retailers, then one would think that there would be much greater collective action by that set to improve security at the point of sale. It is my understanding in the ecosystem, the reason why you see a lot of fraud push back, particularly the account takeover, identity theft, etc., is the notification happens to the issuer, the issuer goes to the retailer through its merchant processor to verify whether the appropriate checks were made when accepting that payment and—failing that verification—the chargeback procedure puts the onus of responsibility back to the retailer.

One of the ways to solve that problem is to increase authentication at the point of purchase, so the person who has the card has a dual or even three-factor authentication procedure to keep the retailer in good status.

What's happening in the UK chip and PIN environment is truly the risk now is borne back to the consumer because of the multiple authentication systems that occur when a chip and PIN card is actually accepted. That's good for banks, that's good for retailers, maybe it's questionable whether or not it's good for cardholders,

but it at least *puts* the onus of responsibility for safety, soundness and security of those card payment instruments back on the people who have them in their purse or wallet.

But we don't see that in the United States. We continue on with the same retail acceptance model we have largely because, I would believe, no one wants to bear those costs. If 90 percent is being borne by merchants, it is amazing that we don't see chip and PIN becoming a much greater argument for investment within the retail POS landscape. There are some strides. I know Wal-Mart does a very good job of terminal driving to PIN acceptance for a couple of reasons, both for cost-efficiency and for authentication reasons too.

Mr. Greene: Stuart, if you and Dick Porter were looking to take some research topics from this session, maybe that's one: What is the role of the Fed in helping to allocate responsibility for assumption of loss, given where the burden currently lies today in the incentive structure? And it's increasing.

Mr. Taylor: I've spent the last year working with small retailers on data security. PCI, as we all know, is one of those amorphous moving targets that is more stick than carrot. What I'm finding is there is a huge degree of noncompliance in what we call the Level 4 merchants. We are talking about 5 million merchant stores out there that are not compliant.

The reasons why there is pushback are multiple. One is—the Verizon study was quoted—while about 40 percent of the breaches occur in retail, 97 percent of the *cardholder* breaches occur in financial institutions. So, in other words, retail only accounts for 7 percent of the card accounts that are compromised. When I talk to my members and they're spending, on average, $20,000 per store to become PCI-compliant, last year their pretax profit was $40,000. With $20,000 a year to become PCI-compliant, they're finding it much more effective to self-insure. If you take my industry to the n^{th} degree, it's $1.5 billion.

We are being mandated by the five card brands to pay $1 per outstanding card for security. At the end of the day, if you still get breached, you're not in compliance and all of the Account Data Compromise Recoveries (ADCRs) and everything else are going to come back down on your head.

I guess my question back to you guys is, first and foremost because we are talking about the Fed's role, Isn't that a role of the Federal Reserve to protect what is becoming the next generation of currency called plastic and the integrity of that currency? Taking a lead role in determining what that data security standard is going to be is part of a national framework that also includes health records, personal records, data security for electrical grids, etc. Shouldn't there be a national conversation that includes, as a subsection, the financial sector on what the national data security standards are going to be? The main reason is there is another factor that's coming in, and the states are individually legislating data security policies in the absence of a federal policy. So, if you are a multistate retailer, you now don't know

how to comply with any of the state legislation that's out there. What we have is a Tower of Babel. There is an absolute role for the Fed to come in, take a realistic role, don't tell retailers to go to triple data encryption standard (DES) when there is not a problem on single DES output. Take a more rational approach. And also you need a third party who is going to be willing to throw out the existing antiquated rails.

Mr. Greene: We don't have a Fed representative up here, but there are lots in the audience. Anybody want to speak to that?

Mr. Weiner: I might say that the next session, of course, is on the Fed as operator and, by that, there are some central banks around the world who, in fact, are maintaining security databases now. That seems to be an extension of that idea, so perhaps we can get into that in the next session.

Mr. Greene: Paola, one of the things you've been talking about is the need for more international collaboration.

Ms. Masi: That's one of the aspects we can add to the debate on fraud. As overseers, and from a system perspective, we are trying to agree on and build a database on fraud at the international level. At the European level, we are trying to agree on a common definition of what fraud is, how we can properly measure it, and who is the authority/institution allowed to store and use confidential data. We, as central bankers, are trying to understand how to build up a reliable and "official" database on fraud, since the available information is too often dodgy and the evaluation of the impact of the fraud on the economy is very different. We are working on this, at least at the European level (as Wiebe Ruttenberg can testify), as a part of the project to have a single database on cards payments.

I must tell you it is a difficult project. We are talking to different categories of stakeholders of any card scheme, starting from issuers and acquirers, and it is really hard to strike the proper balance among conflicting interests; moreover, we have to define how to compare between different nations and between different kinds of card payments. That is why I believe we need to increase our effort at the international level—not only at the European level—to understand, standardize and collect reliable data on fraud. I think also the World Bank should be involved in this effort, and together we can address the question.

Mr. Greene: So international cooperation is needed, but I think your point was, even within the United States, there is plenty of room for improving the standards. The story as I understand it so far is the risks in the retail system are growing, they are growing perhaps by leaps and bounds as a result of some of the new products, the new technologies, the new entrants coming into the space and yet retailers who bear the disproportionate burden and cost of all this are not given the proper regulatory structure to rely upon. They don't know how to operate. They are not sure about the rules of the road. So, is the role of the Fed domestically and similar central banks internationally to help pave that road?

Mr. Taylor: Databases are great. But that is all rear-view mirror. Essentially what the retailers are involved in is a chase-the-crook type of investment strategy,

which is as soon as we find out some new breach, everybody gets lawyered up. Two years later we find out what the breach was and then we can't even react to it because the same exploit has been replicated. It's all because we're trying to incrementally fix a system that really needs a fundamental redo.

For instance, why isn't there a PIN on every transaction? In my market, the solution is to have somebody put in their zip code. If customers can't stand PIN, why do they like a five-digit zip code?

Mr. Eckert: I would like to jump in on that and reiterate that my views aren't the express views of HSBC on this front. However, this is precisely where a regulatory intervention could be very helpful because it is a shared problem for which there is a clear market failure. We're all bearing costs. It's costing the consumers in terms of hidden costs to manage this, and we don't have a lot of joint cooperation among all the parties that are victims to this fraud playing well and nice together.

For example, we have third-party databases where banks have come together in a multilateral fashion to try to share information. But it is voluntary. Early Warning Systems is one on the checking account side. Another one is Certegy Check Services, which is run by Fidelity Information Services, but it has its challenges. First of all, it's based on legacy plumbing information (checks, which we all know how voluminous checks are nowadays), but then secondarily, it is voluntary participation by usually the largest banks, but not necessarily always.

Fraudsters know this. So what do they do? If you looked at some of my subsequent pages that I didn't share in my opening remarks, just as soon as we have a countermeasure to try to help detect and eliminate this at least from the issuer front, then there are five websites that list those institutions that choose not to participate in those Early Warning Systems and ChexSystems to tell the fraudsters where to go! That is clearly a market failure, where you could see a regulatory body, such as the Fed, start to set standards for the betterment of market efficiency as opposed to intervening in a way that could potentially create some unintended consequences.

Mr. Van Dyke: A couple of points: 1) PIN versus signature has been talked about a lot, so I'll just say from our data—and we have seven years' longitudinal survey data—it's pretty clear. The more knowledgeable you are about technology, the more you prefer PIN. The less knowledgeable you are about technology, the more you prefer signature. So the group that prefers signature is going out of the economy. Truly, I think it's pretty straightforward.

This issue of how we would implement these systems, and I appreciate what you said about people entering their zip code, so why wouldn't they enter a PIN? That's a good way of characterizing it. One of the challenges is these crimes we are talking about are inherently complex. Just on the surface, there are two crimes within this one crime of so-called identity theft—steal the data and use the data—and there is often a supply chain of criminals. They are international. They are the

person next door. It's everybody.

Where I think we fall short, because it's hard to take boring research data and convert it into action with these multiple crimes, multiple criminals and evolving things, is that we look at things like malware and Trojan horses and we stop right there at the first crime, which is security. We don't consider how people can use this in transactional fraud. You really have to keep both scenarios alive at once and involve the identity holders and the multiple participants in the supply chain of payments.

Mr. Peirez: I find myself agreeing with many of the comments on this issue, although the Fed's role in terms of what it could study and do is probably broader than what's been discussed because the 90-10 discussion is frankly the exact opposite of what our data show in terms of who is bearing losses. No disrespect meant, Jim, I usually agree with most of your numbers. However, with this one I don't see it. The Fed could do a really great service by trying to identify what costs are being borne by whom. That would be fabulous information for all of us.

Frankly, Peter, to your point. We do provide interchange incentives based on authentication method. It is one of the core rate-based decisions we make. So, if we could get better information on who is bearing what costs in that regard, that would help us independently set our prices in the way free markets should. That would be great information to have. But I don't think we should assume one side is bearing more costs and then start studying how to create incentives around it. We should study who is bearing what costs *first*, then we can try to decide where it should be placed.

And, then, just for the sake of argument on the PIN situation, PIN with chip is a very secure system worth discussing. Dan's points are right on in terms of the cost and the incentives. Personally, I would hate to see us push PIN with magnetic stripe more. It is actually quite insecure and opens up ATM fraud in a way I would hate to see. It's what the Europeans have started to experience, particularly the United Kingdom, based on how they still mag stripe their cards with PIN. I would discourage us from thinking of PIN as a panacea. It's not. Frankly, my zip code is public information that anyone could find and my PIN is not. That is why I enter my zip code happily at the gas station. I wouldn't want to enter my PIN—personal knowledge. It's research-based.

Mr. Eckert: I actually like Josh Peirez's comments, because one of our challenges is you deal with the limited data that are available. What you are suggesting is a system whereby we motivate more participants, financial institutions and merchants to share data.

I agree on the other. The better the quality of data, the better the quality of the decision. I feel pretty good on the numbers we have, but we need more.

Ms. Allen: I want to go back to your question of the role of central banks. I see three important roles that also need to be in the mix. First, I do think the Fed

needs to take a much stronger role in consumer protection. There may not be a need for a consumer protection agency, if the existing regulatory agencies took a much stronger consumer protection position.

Second, the Federal Reserve Board has taken a leadership position in Washington around the cyber-security issues. It's very complex. There has to be global law enforcement, financial institutions, technology providers, and telcos at the table. Again there is a stronger role the Fed could take.

Third is this concept of nontraditional players—nonbanks—acting or looking like banks or doing financial services-types of transactions or activities. Maybe it's the *activities* that should be regulated, not necessarily the entities, and all of that should be done in the name of security and creating the safety and soundness we need to preserve in the United States.