Managing the Threats to Data Security

Moderator: Tracy Kitten

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mr. Marshall: That scares me!

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

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

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

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

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

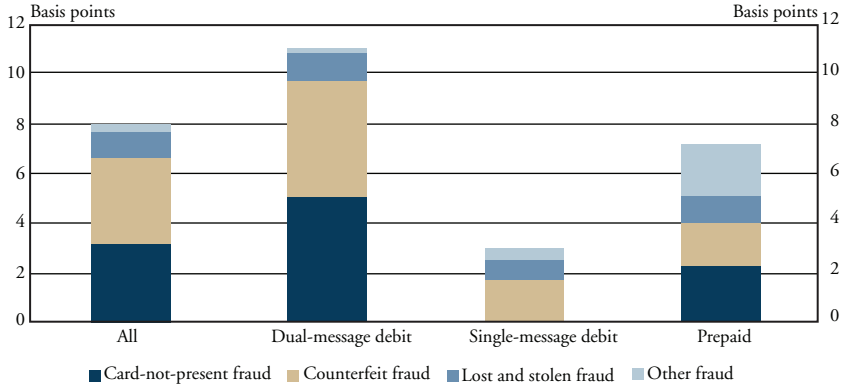
Further, technologies we have been talking about, in particular EMV, tokenization and encryption, are not created equal across all proprietary specification groups. I think that is a huge concern for merchants deploying a mobile strategy because there are rules out there, at least the card brands in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

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

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

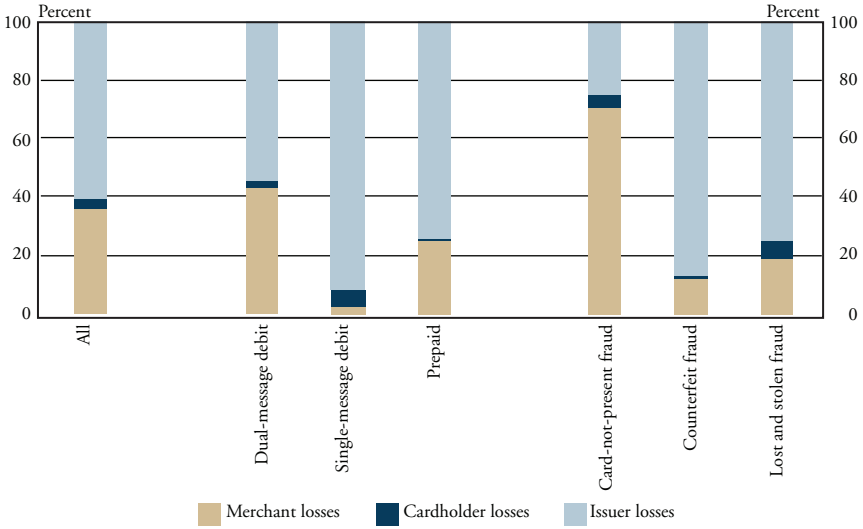
Mr. Carney: I am going to lend a QSA perspective to some of the topics we have been talking about, particularly in three different areas—PCI data, post-data breaches and third-party vendor risk assessments and management.

Chart 1
Fraud Losses as a Share of Transaction Value and by Transaction Category, 2013



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

Chart 2
Fraud Losses by Transaction Category and Fraud Type, 2013



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ms. Kitten: What do you think, Vernon?

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

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

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

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

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

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

Mr. Marshall: Yes, exactly.

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

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