



Remarks by
Ellen Richey, Chief Enterprise Risk Officer, Visa Inc.
at the Visa Security Summit, March 19, 2009

I'd like to open by thanking each of you for being here – especially those of you who travelled from other locations around the globe. I'd also like to thank you for your contributions to advancing data security since our last meeting. In our business, as elsewhere, negativity dominates the headlines. But we've made substantial progress since we last met at the 2007 Visa Security Summit.

First, corporate leadership has risen to the challenge of making security a strategic priority. In a recent Visa-Economist poll of global executives, 75 percent said a C-level executive is now responsible for payment security within their company. Second, we're showing results. Thanks to massive investments and innovative solutions, fraud rates in our industry remain near all-time lows. Third, we have made real progress in expanding adoption of the Payment Card Industry Data Security Standard, with 90% of large U.S. merchants now validating compliance. Fourth and finally, we've heard good news from here in Washington. President Obama has created a National Cyber Advisor post and committed to increasing focus on cyber-crimes, in partnership with industry.

In this ongoing security battle, partnership is the winning strategy. But despite our progress, the reality is that public perceptions of data security continue to be shaped by visible exceptions where data is lost. One such event was the recent compromise at Heartland Payment Systems. I'm sure that everyone in this room has read the headlines questioning how an event of this magnitude could still happen today. The fact is: it never should have.

As we've all read, the company had validated PCI compliance. But it was the lack of ongoing vigilance in maintaining compliance that left the company vulnerable to attack. Based on our findings following the compromise, Visa has taken the necessary step of removing Heartland from its online list of PCI DSS compliant service providers.

In addition, we are activating our account data compromise recovery programs, which are in place to protect our system and help issuers recoup some of their losses from compromise events. And Heartland will face fines and probationary terms proportionate to an event of this magnitude. While this situation is unfortunate, it does not make me question the tools we have at our disposal – in fact, it makes me resolved that we all should be redoubling our efforts to use every one of those tools effectively.

MAINTAINING SECURITY INVESTMENTS IN A DIFFICULT ECONOMY

Of course, events like Heartland grab headlines. But today, the headlines about our dire economic landscape may actually be the bigger threat to payment security. As The Wall Street Journal recently put it: *"The bear economy is creating a bull market for cyber-crooks."* Common sense suggests that a poor economy and a bleak job market would increase desperation – and creativity – among would-be data thieves. And sure enough, security and law enforcement experts confirm that cyber attacks on consumers and businesses have intensified in recent months.

Javelin Strategy and Research recently reported that identity theft incidents in the U.S. were up 22 percent in 2008. Visa's own data security experts have detected increases in attempted scams and attempted system intrusions: not just their frequency, but also their sophistication.

Unfortunately, these increases are taking place at a time when there is intense pressure to cut costs. When every cost center is being targeted for reduction, we can safely assume that data security will not be immune. We should all be concerned when businesses connected to the payment network are under pressure to shortchange security measures. I expect those of us in this room would all agree that this kind of cost-cutting is short-sighted and dangerous. But we have to acknowledge that others in our organizations may not see things our way – or may feel they have no choice.

In response, we must increase our presence as educators and advocates for data security. If we cannot convey the urgent need to maintain investments in payment security – particularly in today's environment – years of progress in building consumer trust could slip through our fingers. The bottom line is that we must be more efficient, more vigilant and more convincing than ever to ensure that critical investments in security continue to be made. It is the only way to assure businesses and consumers that they can trust our system to deliver value, safely and securely.

PRIORITIES TO SECURE THE FUTURE OF PAYMENTS

So, where should we focus at this challenging time – when every penny counts and the integrity of the payment system is being questioned in the media? The answer is that we must continue to work both collectively and creatively. No one of us can solve the security challenge alone; but by working collectively we can maintain our greatest strength: the power of thousands of companies working together.

In our strength, however, lies a potential challenge. By its nature, an open loop network like ours is complex – progress is made through many steady, incremental steps. There is no “silver bullet” in payments security – and likely never will be. And so as criminals get more sophisticated, we must also get more creative in building multiple layers of security – in technological innovations, in partnerships, in business processes – to ensure that we continue to stay one step ahead.

As we engage in discussions today, I suggest we ground our thinking in three fundamental tasks: Preventing criminal attacks, protecting our system when they do occur, and responding immediately to minimize their impact.

As an industry, we've made great strides in responding – helping consumers and minimizing the impact of fraud after the fact. But I believe we can do more in our efforts to get “upstream” of fraud. More specifically, I see four priorities that can help shut down criminal activity before it starts.

First, we must make sure we are actively managing the threat of compromises, and doing so in a way that does not unnecessarily burden business.

Recent rumblings about the demise of the PCI DSS are not only premature; they are dangerous to long-term security. Despite recent negative commentary, the PCI DSS remains an effective security tool when implemented properly. Simply put, it is the best

defense against data theft available today. As we've said before, no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach.

But the standards can only significantly reduce the risk of breach if they are fully implemented and consistently followed. Let there be no mistake, it's not validation that provides protection – validation is only a snapshot in time, like a financial audit or a health inspector's report. It is the ongoing commitment to maintaining compliance – 24 hours a day, 365 days a year – that protects an organization from suffering a breach. And, finally, PCI DSS is not meant to be exhaustive. The standards provide a strong foundation – and the best security strategies build on that foundation to create a multi-layered and evolving defense.

In short, increasing validation levels is important. But so is increasing the understanding of the big difference between obtaining validation and maintaining security. At Visa, we recognize this is a priority. You can be sure we'll be working to increase the number of ways we can help raise awareness on this critical point, and ensure that security efforts don't stop with an assessor's report.

Let me return for a moment to that fundamental first step. As I said, PCI compliance validation among the largest U.S. merchants has grown to about 90 percent. And 99 percent have now certified they don't store prohibited data. That's good news. But the numbers outside the U.S. are much lower and require immediate attention. That's why Visa has announced deadlines for global PCI DSS validation, creating a consistent framework for compliance among merchants, service providers and their agents worldwide. By September 30 of this year, Visa has asked large merchants all over the world to validate that they do not store prohibited data. Then, by September 30, 2010, we are requiring all Level One merchants globally to validate full PCI DSS compliance.

At the same time we seek to grow PCI compliance, however, we need to recognize effort being put in place to help mitigate systemic risk - both here and elsewhere around the world. That's why we support the PCI Security Standards Council's creation of a prioritized approach to the PCI standard, and will be building upon this approach to enhance Visa's compliance validation programs globally.

In addition, we recognize the value of security measures that are not currently part of the PCI DSS – specifically chip technology and encryption. And we are working on an approach that would allow merchants to satisfy some of our compliance requirements through the application of chip or encryption tools. With a prioritized approach, these additional security measures – such as end to end encryption – can complement PCI, and help organizations meet the standards in a more flexible way. We'll be sharing more information about the specifics of Visa's prioritized approach this spring.

Second, we must more actively engage consumers and empower them to help protect themselves.

In the old days – like 2003 - our industry could take care of security for consumers and simply assure them they were protected. After all, we know that compromised data only leads to fraud in a small percentage of cases. And consumers enjoy our zero-liability protection, which essentially absolves them of financial liability for fraud.

But consumers today are not just worried about fraud. They are fearful about who might be using their personal information — and where and when. These consumer fears are real. They impact behavior. And they must be accounted for in how we approach system security. So in today's environment, consumers need – and expect – to be a part of the solution.

According to a 2008 Javelin study, just over half of consumers view the responsibility for protecting financial accounts from fraud as equally shared between themselves and their financial provider.

We agree that everyone has a role to play in securing the system – including consumers themselves. And so, while Visa and its issuers already monitor and risk-score transactions, we can achieve even more by providing consumers with additional tools and putting more information in their hands. In two new programs, Visa is seeking to provide the right information at the right time.

The first is our recently announced Transaction Alert system, currently available to Chase cardholders with Android mobile devices, and coming later this year to all Visa issuers. In this program cardholders receive near real-time notification of purchase activity to their mobile device or email. The consumer can personalize the alerts – by transaction size, online purchases or foreign-currency transactions. Armed with this kind of information, cardholders can help monitor usage on their accounts and stop fraud.

The second program, still in development, relates to Targeted Acceptance services, which would allow consumers to set personal limits on how their cards can be used – such as dollar amounts, geographic limits or merchant segments. Any transaction outside the limits would be automatically declined – before fraud can occur. This service is already available on commercial cards, where Visa acceptance controls help businesses manage their expenses.

We think the time has come to explore extending the same kind of control to consumers. And by using Visa's system capabilities, we believe we can make the process easy to use for cardholders and easy to implement for issuers, with no additional software required. Of course, these are just examples of the kinds of tools that enable cardholders to take a more active role in security. We encourage the industry to continue pursuing consumer-directed technologies that make cardholders part of the solution.

Third, we must increase collaboration across the payments system – to close security gaps and share critical information faster.

Every day, Visa works across a broad spectrum of parties within the world of security – lawmakers and law enforcement, partners and processors, clients and competitors. In fact, we work with many of you in this room, in one way or another, on a regular basis. We do this because we know collaboration is critical to our mutual success. And in collaborating, we know nothing is more important – or more helpful – than sharing information. Let me give you an example of what I mean.

Visa has access to a great deal of useful information in our systems – information we make available to help Visa issuers make better decisions about authorization management. In 2008, Visa launched Visa Risk Manager in the Americas. This is an intelligent decisioning service for issuers. Powered by our VisaNet network and our Advanced Authorization service, VRM provides issuers with automated tools that help them respond to fraud as it occurs, including criteria used to make real-time decisions on the highest-risk transactions

and effective ways to examine suspicious transaction activity. There is a demo outside that provides more details about this service.

Another area in which information sharing is critical is e-commerce. Visa has already invested in helping online merchants reduce fraud through address verification matching and use of CVV2 codes on the backs of cards. And, we've developed authentication measures for situations when neither the card nor the buyer is present.

But at the last Visa Security Summit, Meg Whitman of eBay called on the industry to increase information sharing with merchants. We thought that was a great idea. So we began to develop a version of our Advanced Authorization risk scoring service, tailored for online merchants. We now have a model that we believe can predict the likelihood of an e-commerce transaction resulting in fraud and we are currently in the process of validating that model. Our objective is to help merchants "score" each e-commerce purchase for its fraud potential. That score can give those merchants more and better information they can use to prevent fraud and protect themselves. By making the information we have available, we can help others use it to stop fraud. That's something we all can seek to do more often.

Fourth and last, we must continue to reduce the value of stolen data, through investment in new authentication measures.

While we all agree on the need to protect data, the future lies in finding ways to make stolen data unusable. For us, that means authentication. Many parts of the world have adopted chip-and-PIN as a primary means of authentication. Others, like the U.S., rely primarily on mag-stripe technology supplemented by advanced risk tools and centralized processing.

I am often asked why the U.S. doesn't adopt chip. The answer is that it's not a matter of adopting or not – but a matter of "when" and "how." In the U.S., we're beginning to see adoption of chip technologies first through contactless payments. Let me be clear: from Visa's perspective, chip technologies – both contact and contactless – can add an important security layer. They also offer additional benefits for cardholders and retailers, like convenience and speed. So we can and do fully support chip technology.

But we recognize that there are differing needs, threats and infrastructures in different parts of the world. As such, we continue to believe that there is no "one-size-fits-all" answer. Chip adoption is best achieved through a market-by-market approach, based on how and when a market will support it.

The debate about how and when to adopt chip may continue. But one thing is clear: the right long-range goal is to make data unusable by criminals – reducing the incentive to steal it. And at Visa, we believe the best way to get there is by introducing dynamic data into the transaction authentication process. Chip is one way to do this. And we're exploring others. But in the meantime, we are also looking at other creative avenues to reduce risk.

During the first of our panels today, you'll hear more about two interesting pilots that show how unique bits of information can also be used to stop fraud. One is a challenge-response pilot at OfficeMax stores in the U.S. By asking consumers to respond to a question at the point of sale, issuers and retailers can reduce fraud, especially in high-ticket environments.

Another is from Fifth-Third Bank, which uses innovative mag-stripe technology. Each mag stripe contains unique physical characteristics, like a finger print, that can be used to verify the digital identity of the card being used. You can also see more about both of these

solutions at the demo tables outside. While these ideas are not ready for roll-out yet, these kinds of creative solutions can help make stolen data useless at the point of sale.

Now, more than ever, payment security is an evolving and complex puzzle. There is no magic “code” to be cracked. Frankly, there never will be. In this arms race with criminals, the solution is to apply many solutions – in a layered approach. Every layer is important: PCI compliance is important; encryption is important; consumer engagement is important; collaboration is important; authentication is important. In fact, consumers increasingly expect the companies they deal with to be doing all of the above and then some.

In line with this idea, we have another layer to add: I am proud to announce that Visa has joined McAfee’s Initiative to Fight Cybercrime, an effort that will assemble global leaders to develop concrete action plans to reduce digital crimes. You’ll hear more about this important project from Dave DeWalt, CEO of McAfee, later this morning – and I encourage you to champion it within your organization.

As you all know, maintaining security is a relentless and unforgiving job. Every failure impacts us all – and reflects on us all. But success is equally shared. And our collective success will come from the steady and incremental steps we take together. That is the best and only way we’ll ultimately stay ahead of criminals. As I mentioned earlier, we see a positive trend towards better data security within the payments industry. But there is also a dangerous undercurrent of economic pressure that can threaten our efforts to stop criminals. Our best advantage over criminals is our ability to work together. So let’s do everything we can to build on that strength – starting with today’s discussions.

#