Nonbanks in the Payments System: Innovation, Competition, and Risk

2007 Payments Conference
Federal Reserve Bank of Kansas City
May 2-4, 2007
Santa Fe, NM

Session 5: Risk
Panelist Remarks
Moderator: Avivah Litan, Vice President and Distinguished Analyst, Gartner, Inc.
Panelist: Jean Bruesewitz, Senior Vice President, Visa U.S.A.

Ms. Bruesewitz:

Thank you, Avivah. Good morning.

Let me give you some Visa statistics from a worldwide perspective. We had 1.5 billion cards at the end of 2006 worldwide, 503 million cards in the United States. At the end of December 2006, we look at 6.3 million acceptance locations in the United States and 24 billion worldwide. The total volumes worldwide that are processed through Visa are $4.5 trillion. It is a huge business. We are very invested in everything around the payments system. We are extremely invested in risk and security.

The balancing act we have to work with all the time is balancing between convenience and security, ensuring consumers get to do what they want to do, which is to purchase goods, get access to cash, and go on about their lives and not be too dependent upon the consumers to have to run security management for us. I think there is a big difference there from a European perspective. If you look at how we take a look at our security strategy, this is a water-balloon effect.

What you have is you are going to find a way to close a hole over here. It is going to push the fraudsters another direction. So, how do you keep working on different ways, different methods, and different points within the transaction cycle to be able to manage the risks that are out there?

When we look at this, we look first at securing the payments system. I would tell you in—now it has been so long—December 2000 when Egghead was hacked, it became very clear, very quickly to us at Visa that we were not looking for large events. If you looked at the type of fraud detection we were really focused on, it was an account-by-account, transaction-based fraud detection approach. So, you had a whole new way to start to look at these things. We set about immediately on, what was CISP which has now turned into PCI, data security standards that we have gotten agreement from the payments schemes on, to take a look at how people are managing data within their systems.

If you think about it from a rule's perspective, at Visa we always had the rule that the data had to be protected, but we were in a different environment. You were in mainframe computers. There was no access wirelessly. You had to have a lot of money to be able to get computer access.

You look today—and one of the handouts yesterday showed the cost of computing and how it has gone down—now it is very easy for

everybody to get enough computing power to do things. So, we have worked very hard from a data security standpoint to say, "Let's get all of the constituents up to speed in securing their data to try to stop the leakage of data in the payments system."

Along with that, at Visa we have put together a payment application best practices. What we have found is that developers' payment applications and the ability of software to store more and more data have helped us out by storing more and more data, including track data that should never have been stored in the first place. What can happen is a retailer can not even be aware that is going on. So we are starting to see PCI work. But what we are also starting to see is smaller merchants that are being hacked because the software they are using is storing transaction data. There is a push. Now, the biggest risk is your top locations, where your large amounts of data are. But it is pushing them to look at smaller and smaller merchants. So, we are having an effect there.

As we look at securing the payments system, we have a lot of tools that are in place on the card in the mag stripe. CVV, which is the encoding on the card; CVV2 on the Internet; and Address Verification Service, of course, if all that is stored in a database then that is going to be put at risk too. But you still have all those tools to work with.

So, then we approach that in a way you have to be schizophrenic and never believe you will ever get this secured again, then you look at

how you monitor, identify, and prevent the fraud. So, we have a very integrated network. We have brought the Plus System, which is the ATM system, Interlink, and Visa, into the Visa Net Payment System because we wanted to ensure one of the most important things is to get real-time, in-flight authorization and fraud detection to make it available to issuers, so at the time they want to decide how they are going to handle the transaction, we have provided them with all the information we possibly can to help make that decision.

If we look across that we first have the authorization system. The electronic authorization systems were the first risk detection systems. We look at authorization. We have advanced authorization, which is our fraud detection system that is looking at the transaction standpoint. It is looking at the account level, it is looking at an event, and the risk of this account in the type of event that it was in, and what we are seeing from a fraud perspective so we can provide issuers with all that information.

We have ID theft prevention systems and tools that we provide out with a fraud-reporting system. Why this is important is, for a long time, we all felt very secure about PIN fraud. PIN fraud is not going to happen and PINs are secure. We know that is not true now. We are bringing in PIN fraud as fast as possible. Our fraud detection systems are already built across all types of transaction fraud.

New authentication approaches—Verified by Visa. In the first place, is there a liability for the consumer? Verified by Visa we have in the market for non-face-to-face merchant locations and for consumers.

What happens is that we are seeing the fraudsters take over the accounts. This gets back to how do I know who the consumer is when they contact me and they get into their own account or the fraudster gets in and goes forward to get Verified by Visa? That is the risk we are seeing. What we are not seeing is a breakdown in the system itself.

So, you have all those tools in the middle of the transaction and then managing the impacts of fraud. That is from fraud investigations to breach management and coordination with law enforcement and to really try to control the movement of funds. We look very much at how you stop it at the point of sale and how you ensure that whatever tools you are using are as accurate as possible. What you want to do is not impact the consumer and to be able to stop the fraudster. It is very hard to collect the money. If it is taken out of an ATM in Eastern Europe, you are never going to see the money back. The first thing is, How do you stop them from getting the money?

Maintaining trust in the Visa payment system is real important. We do an awful lot of education to the consumers because it is important. There are a lot of fraud controls, a lot of telephone calls they receive from their banks to validate where they are, and they need

to understand and have an understanding that is for their benefit and their bank is following up on things. We work again with cardholders, merchants, legislators, and regulators in creating an environment of partnership.

We agreed with MasterCard, Discover, JCB, and American Express to put a PCI Security Standards Council together. That is up and running. We have agreed to the same standard. We have standards around PIN pads and now we are going to take our payments application standards that we have been working on into that group to try to expand that even further.

We work a lot with law enforcement. We work a lot with other payments networks. That is how we eliminate track data and how we render the data useless.

Then, of course, we start out with consumer protections. We are looking at zero liability for consumers, VVV that we have available. Lots of fraud monitoring: the codes, the ID theft, a lot of robust systems, including the whole dispute process, that we are able to hook the banks up worldwide to be able to handle disputes and protect consumers at the same time.

But it is something you have to continue to work on and continue to change. There is no reason for the bad guys to try to get in and decrypt our information today because, quite frankly, the encrypted information, when they get it out of a database, can be used.

Therefore, why would you have to decrypt it? The tighter you get from a data perspective, they are going to start to look at new ways to get at the money because that is their goal.

Avivah talked about out-of-wallet static information. It is one of the things we are built on. That static information, of course, is everywhere. You are never going to get consumer information back in a box. You are going to have to believe that you have to look at what you can validate, how you can get out-of-wallet information, how do you look at behavior, and continue to build tools sets and layers of security to protect the industry.

Thank you.

Ms. Litan:

Thanks. So, Jean, if the controls are in place—and I know it takes a long time to roll all these controls out—why do we see all this fraud taking place after a breach? In other words, what is the time lag? What goes on if someone steals 40 million cards from card systems or TJX? If there is such good communication with the Visa issuers, why is fraud taking place?

Ms. Bruesewitz:

First, I want to put fraud in perspective. If you look at fraud and even gross fraud in the Visa system, we are flat from 2005 to 2006 as a

percentage of sales. That does not mean it is a small issue, but the sales have continued to rise at the same rate as the fraud we have had. What you see and what I think we are seeing is that a lot of the fraud that we have been taking in the system has been part of breaches. We had not identified it as breaches.

As far as how long it takes for the fraud to occur, on an overall basis, we see less than 1 percent of the accounts that have been involved in a breach that actually have fraud on them, which is the reason why you do not want to rush out and reissue every card you have. Because in fact, we do not see fraud at that level. Again, this is why in the stream, how do you manage against this type of risk?

Ms. Litan:

If it was so mild and such a small percentage, then why are three bank associations suing TJX for the cost of card replacements?

Ms. Bruesewitz:

Those are operational expenses too, without the fraud. So, if the choice is made to replace the cards, there is a huge operational expense to do that. Not only that, there is an impact to the consumer. If you are a consumer and you have had your card replaced two or three times by your issuer, it may have an effect on what you do in the future and how you use your card. A big expense.

Ms. Litan:

If you look at all the tools at your disposal, could you describe what you think would be the ideal security system that you and your participants would roll out?

Ms. Bruesewitz:

If I could tell you, I would not be here. I would be very rich if I had the ideal security system. You have to continue to look at it. We are doing a lot of work on authentication. If you look at what has happened over the years in the payments system, things work for so long. Then technology changes, people get smarter, you have to add new tools, you change your tools, and you have to maintain the convenience. Again, you have to balance the amount of risk you have in the system with the convenience to the consumer. If you make it too hard, they are going to fall back to other methods of payment, which is not what we want to do either.

Ms. Litan:

When you talk about the risk versus the convenience, you are really looking at it from the issuer's side, aren't you? When Visa and MasterCard talk about the fraud rates, they are talking about the fraud to the issuer, not the amount the merchants experience.

Ms. Bruesewitz:

I was talking about gross fraud.

Ms. Litan:

Could you talk about sharing information with merchants—what the policy is after fraud takes place—and also about the systems you have available? You talked about the issuers a lot. What about the merchant side?

Ms. Bruesewitz:

From a merchant's side, if a merchant in a face-to-face environment has followed the rules they need to follow, the liability is really on the issuing side. In a non-face-to-face environment, the merchant has a much better chance to know that consumer, if they have shopped there before.

The issuer has the information available to them that comes in through the transaction. What we do there is there is Verified by Visa available to merchants. If they put in Verified by Visa, the liability is shifted on Visa transactions to the Visa issuer. We provide, from a risk perspective on a transaction basis, all the information to the issuer to help them make their decision as to whether or not they want to authorize the transaction.

Ms. Litan:

I do not mean to get into too much detail, but I have always been very interested in knowing why the banks are bearing the cost of counterfeit fraud if it is the merchant's responsibility? I have been hearing from issuing banks that counterfeit fraud is going up significantly, and they are having to pay for it. But the supermarket, for example, saw a good card, they got a signature, so why are they able to shift back the fraud to the merchants under the new PCI rules? With the new Visa rules, I understand the merchants have to pay the direct fraud costs, even though they did everything they were supposed to do. You look a little perplexed by the question.

Ms. Bruesewitz:

I am, so let me answer what I think you are asking me and then tell me if I did not do that. Are you talking about a breach at this point?

Okay, so from a breach perspective, if there is a breach and the merchant was found not to be PCI-compliant, then we have a process. There has always been a compliance process. But we have a process of—ACR, thanks—Account Data Compromise Recovery Process that has been worked out between issuers and acquirers, where we look at how liability should shift because of the breach between the issuer and

the acquirer. It has been worked out as a way where the constituents—members of Visa—have looked at how that should be shifted.

Ms. Litan:

In terms of PCI, you said you are making progress. But what is your honest opinion of the feasibility of 80 percent of the merchants becoming PCI-compliant in the next two years?

Ms. Bruesewitz:

Well, I would tell you that the risk people are working extremely hard to try to make that happen. You have to always believe, and it is a dynamic environment. All you need is a software change that opens a port that makes you vulnerable again. It is one of those things that you have to always believe that you will work to try to make it 100 percent. And, secondly, you will believe that you will never quite get there. That is why you have to have a layered approach and have other directions that you take to help secure that data and make it useless.

Ms. Litan:

One last question. When Visa goes public, what do you think it will do to all these security initiatives? Do you see anything changing two years down the road?

Ms. Bruesewitz:

I cannot comment on the future of Visa. So, thank you, Avivah.

Ms. Litan:

How about your personal opinion?

Ms. Bruesewitz:

I have no personal opinions on that.

Ms. Litan:

Okay, Roy, you are next.