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
Moderator Remarks
Moderator: Avivah Litan, Vice President and Distinguished Analyst, Gartner, Inc.

Ms. Litan:

Thank you very much, Ross. I personally thought your paper was really excellent because, when I look at the data that I collect, the main issue I see where regulators should play in is, Where do consumers go when they can't get their money back? And they are getting scammed, and I will talk about that. That seems to be the big issue: They are not protected and there is no party that is incented to protect consumers financially. So, that is where I think regulators come in.

When I look out there, I see two attack vectors that have emerged in the last few years that were not there five or 10 years ago because of the Internet. Thieves have found their way through to the path of least resistance. One of these two attack vectors are the retailer systems. There are about 6 million retailers out in the United States. (I mainly have U.S. data, so I apologize to the European people at the conference. I just do not have the data, but I am sure the numbers are very similar.) So, there are about 6 million retailers in the United States, and the thieves have figured out how to get into their systems, many of the times through point-of-sale systems, store systems, like the ones big retailers such as TJX have in thousands of locations. They find their way into just one of them through wireless Internet access.

The second attack vector is attacks directly against consumers, which Professor Anderson talked about, whether it is phishing or malware. Both these parties are ill-equipped to deal with these risks. These risks have been highlighted. They highlight the weaknesses in the payments systems and the vulnerabilities in the payments systems. They were not thought about when we rolled out retailer credit card accepting systems years ago. No one thought about the fact that cyber criminals can break into our stores. We did not think about malware and phishing attacks when we enabled e-commerce on consumer desktops. That has highlighted all these risks that hopefully we will start to solve.

I am going to elaborate on some of the trends that Professor Anderson talked about—what we have seen and what we see as the solutions.

In terms of the trends out there, aside from those two attack vectors—just to drill in a little bit on consumers—there is a lot more use of less conventional attacks. So, we are seeing a drift away from the phishing attacks that say, “Give me your user ID and password,” to an online bank because the banks have caught on to that, and consumers are starting to catch on to it, to less conventional attacks.

Probably many of you in the audience have gotten phishing e-mails advertising lotteries, sweepstakes, or other types of gift offers. “Here, you can get a Target gift card if you give us your bank account. We will deposit the money and we will give you a prepaid Target gift card.”

To whom do people go when they get ripped off like that? Whose responsibility is it if you fall for a scam? Similarly, with the pharmaceutical scams—“you can get really cheap Viagra here”—that seems to have taken off pretty well, and there really is no one for the consumer to go to when that happens. That is both a bank and a nonbank issue. Whose fault is it if someone falls for a Nigerian scam?

Again, we have seen less direct attacks on online banks. I think the FFIEC guidance on stronger authentication is starting to work. Although, as the professor said, we are starting to see man-in-the-middle attacks, man-in-the-browser attacks, where after you authenticate, whether you use a token, a smart card, or a biometric, the crook can go in and take over the session. There is evidence of that happening in Europe, the UK, and also in the United States, although that does not mean you should not strengthen the front door. But the crooks are taking advantage. They do know how to get around these measures.

Some of my financial institution clients say they see the information being stolen out there is taking a toll on online brokerages accounts, where the thieves use stolen information to steal money. So, now thieves can get into a brokerage and answer questions, take out funds, or open new accounts. The information they may steal from a retailer is now being used at a brokerage firm. That is certainly starting to happen.

We are seeing phishing starting to stabilize. It had a big escalation over the last couple of years. But now malware is taking over as the fastest-growing threat. Malware involves the download of malicious software to your desktop that you cannot really see. They take over your PC. They record your keystrokes. They record when you put in account information. In fact, the estimates are there are about 20 to 30 percent of all user PCs around the world infected with malware. And about 10 to 20 percent of our machines are being used as botnets. Botnets is when they use other people's PCs to launch their attacks.

Of the 20 to 30 percent of the machines that are infected, it is not all keystroke loggers. Some of it is just spyware and trying to figure out what you are doing so they can advertise something else to you. Our machines are really at risk. Those are some of the trends we are seeing.

The biggest issue again is consumer recourse. To whom is the consumer going to go? Whose responsibility is this?

Do not rely on security improvements in the infrastructure. As the professor said, without strong financial incentives, Microsoft was years behind in releasing improvements to the browser. If you look at where does the security belong, it does belong in the Internet infrastructure. It belongs in browsers. It belongs in retailer systems.

But they are not going to pay for it because it does not hurt them. If someone steals data from a retailer, they use the data somewhere else. They do not use the data at that retailer. Microsoft does not really have a very strong financial incentive, other than Linux could beat them because they have better security.

Antiphishing toolbars and the extended validation certificates—I will not bore you with all the technical details—are a good step in the right direction, but they are a slow step, and the crooks have already figured out how to outdo them.

You are not going to get security improvements unless people have strong financial incentives. It is a collective problem. It demands a collective solution. When you hear that, you know that it is just not going to happen.

What is the solution? I agree with you, in part, that you should follow the money, not so much the identity. But frankly, I think you need to do both. You need to have layered security. You should try to identify your users. You should try to put strong access controls on systems, but you cannot rely on that to work. So you need back-end fraud detection. And you do need to help out consumers when they lose money by promoting recoverability of the funds. Identity is important. It is fallible, but you need it for traceability and accountability.

But who is accountable for identity? In the United States, the government is trying to make the Department of Motor Vehicles accountable for identity. They did not get into the business to issue identity cards.

I was mentioning to a couple colleagues last night—someone from the Department of Motor Vehicle Association asked a conference group I was in, “When is the last time you took out your driver’s license for the purpose it was issued?”

We are always showing our driver’s license for non-motor vehicle-related reasons. They really are not in the business of knowing how to vet identities.

Another problem with the Real ID Act is when you get your driver’s license, you have to produce a passport and a birth certificate. When you get a passport, you have to produce the driver’s license and the birth certificate. There are 14,000 versions of birth certificates on top of that. How are people at the DMVs going to figure out which came first and which is an authentic piece of documentation? Until you get the vetting right, you really cannot count on identity.

Also, I agree with you completely, there has been way too much emphasis on the input, identifying the person coming in. How about identifying where the money is going to and the destination? That becomes almost an impossible task. You cannot identify every single receiving point of money in the world, although you can try. It just is not going to happen. So, yes, I totally agree. You should follow the money. It is a narrow and much more achievable goal, and it resolves directly many more consumer issues. Although I know it is not always easy to recover funds, at least there should be more emphasis placed there.

It is a great idea to pay a premium on a finality of high-risk payments. If someone is going to make a final payment, you should have an intermediary, like a cashier's check that you have to pay for to make that payment and the market will be able to handle that. Again, you have to emphasize layered protections. You cannot work only on the front-end authentication. You have to start with identity authentication, you have to have back-end fraud detection in case they get through, and then you have to have what we call "out-of-channel verification" of the transaction. There are several solutions—and I am talking about Internet solutions. There are retail solutions too that Jean hopefully will talk more about in the context of the credit card industry.

Finally, you did not bring this up in your discussion, but you had a part of your paper that talked about how the banks have been pretty good at shifting liability to consumers and merchants. We really do need to stop shifting liability. I think it is better, as you said, to put the risk with the party best able to deal with it. Consumers are not really very well able to deal with the risk. This is a black hole.

For example, let us say that your bank account number gets stolen during a breach against a retailer. How are you supposed to know that? You do not have the information. You do not know what the risks are. You do not know there is a black market out there for information exchange and sales.

Merchants are also kept in the dark. When there is a breach of bank accounts and credit card information, they do not receive that information because of security concerns, etc. But then they are not able to deal with stolen cards properly. Neither party—merchants or consumers—have the resources to mitigate this risk and to solve it.

Let's take the famous TJX example. The payments systems really were pushed out before retailers knew about the cyber attack. I am not saying they should not protect their data. But I talk to retailers all the time, and many just do not have security expertise. Many do not have IT infrastructure expertise. I am talking about the average retailer. They are in the business to sell retail goods; they are not in the business to understand point-of-sale security. They do not even know what is going on in their system half the time. They are already supposedly paying higher fees to mitigate fraud. They are already paying direct fraud costs. They are already paying for PCI compliance. They are paying for breaches and their related fines.

Now, there are three bank associations fining TJX for all their other customer service costs—for closing the account and for card replacement. Maybe it is time for the banks to start seeing that the payments system needs to be secured further. You cannot keep shifting the responsibility to retailers. Maybe it is time to upgrade card security. There are some technologies out there that can help solve card security issues. The bottom line is new risks have shown up at retailers and consumers and highlighting risks in the payments systems. It is not just a nonbank payment provider issue, it is also a bank issue. The risks have highlighted the need to change the payments system, so that if data is stolen, it is useless to the thieves, and also make it easier for consumers to recover money. They are not protected now in many of the scams.

I only have a couple of minutes left, but I did circulate a paper on phishing. If you look through the data, you will see that attacks against banks are going down. The most attacked brands continue to be eBay and PayPal. Phishing attacks are used for different kinds of scams, and consumers fall for those scams. The big, troubling news in the data is that in 2005, consumers recovered about 80 percent of their stolen money; in 2006, they recovered about 54 percent. Of course, there is a margin of error in consumer surveys, but the trend is definitely that they are recovering less of the funds. There are more attacks. Less of the attacks are successful, but when they are successful, they take more money, and it is more difficult for consumers to get back their money.

The message to this conference and to the regulators is that is really where you need to step in. You need to do something about consumer rights and getting back their money through all kinds of payments systems. You also need to look at where the liability should be and who should pay for the risks.

Those are my remarks. Now we will go on to Jean.