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
General Discussion
Author: Ross Anderson, Professor, Cambridge University
Moderator: Avivah Litan, Vice President and Distinguished Analyst, Gartner, Inc.

Ms. Litan:

So, any questions? Yes, Peter? (And Catherine next.)

Mr. Peter Burns, Vice President, Federal Reserve Bank of Philadelphia:

Jim, your very quick comment about TJX in the sales lift and stock price recovery and so forth frankly troubles me a little bit because I have often looked at this reputational risk, stock price risk, as the incentive that was going to drive PCI compliance and other aspects of merchant security. How do we think about this going forward?

Mr. James Van Dyke, President, Javelin Strategy and Research:

Actually, we had a really in-depth analysis. This was a rare time in which we said, "Boy, we are looking at data that simply do not connect!"

We do not say that very often, but sometimes you get properly designed data sources that show a miss between consumers' stated intentions and what they actually do … yet I would say frankly I think

we let ourselves off the hook when we say that the data is not reliable because there is something to be learned from the very dichotomy.

Here is where I see the problem. I have been a big fan of everything, the PCI—going back to its predecessors, CSP and Dirty Dozen—and all things going back over the years in archives. I maintain complete faith, based on looking at the history of the stuff, that consumers' behavior will be changed. It wants to be changed. It is like gravity or some other rule. There is a fundamental property at play here. But people cannot get the information they need to improve their safety through selecting the most safe providers or payment options.

We are doing research right now to get to the bottom of this to explain it. It is my solid belief that the consumer in there says, "You know, I want to penalize that merchant. I do not feel comfortable."

I completely reject the idea that they say, "Well, maybe my security is higher now because there is more scrutiny here."

I do not believe that is true. But I think what is going on is they say, "You know, I am enraged, I am concerned, and yet how do I know I am any safer anywhere else?"

That is what we need to change.

And then they close their bank. And then you get a cost through the industry, but that is more like moving too far down the prevention-

detection-resolution chain, and then you have a problem with cost and benefit.

Ms. Litan:

I just want to add one thing on that. I do see consumers taking it out on their banks, not the retailers. Most consumers do not know about TJX. But they know when their bank calls and says, "We have to give you a new card."

Mr. Anderson:

There is a significant amount of research in this in the security economics community. First, it is well-known that there is a big gap between consumers' stated and revealed preferences and privacy. A lot of people say they value privacy. Most people will sell you their medical records for a cheeseburger.

There is a lot of research on why this happens, and people are starting to understand it. There are time-lag effects and banded rationality effects and so on. It will eventually catch up with us.

Second, there have been a half-dozen or so papers looking at what happens to company stock prices after they announce security breaches. Yet stock prices do drop by a few percentage points and stay down for a few days. So, the effect exists, but it is not a big deal.

As far as consumer behavior with respect to merchants who compromise the data, there was a paper showing you do not lose customers so much the first time you have a compromise. But if you have a second compromise within a relatively short space of time, then you start losing customers.

Ms. Litan:

Cathy.

Ms. Cathy Allen, Chief Executive Officer, Santa Fe Group:

First of all, let me commend your panel. In this risk and security area, you have brought up almost every one of the major issues and challenges that we are facing. So, you did a great job.

I want to go back to something that Professor Anderson said about accountability and shared liability. We in the financial sector are so interdependent on the IT industry, the software industry, the third-party service providers, the telecom industry, and the power industry. In any one of those places, you could have problems with business continuity, but more importantly in access, for information security breaches because in one of those places they can come in.

Yet the only people regulated are the financial institutions. So, a couple of questions for the panel. Should we be regulating third-party service providers; the telecom industry; and, in particular, the IT and

software industry? Or are there other incentives—like insurance or certification requirements or things like that for that industry—so the liability is shared? What happens in the end is the only people the regulators can come after is the financial sector and have us then have oversight on the retailers of the third parties. In a way, that is not really a shared liability. We are at such mercy of the IT industry and the software industry. It is their vulnerabilities that are causing many of the problems that we have now and will have in the future.

So, what are the incentives or views of the panel on regulation?

Ms. Litan:

Who wants to take that?

Mr. Anderson:

Perhaps I can start. If you go back a quarter of a century when I was a youngster, then IBM had a lot of incentives to do stuff to keep the banks sweet because banking was maybe a third of their business. Now, if you look at Microsoft, banking might be a million Windows licenses—the same as Defense? Microsoft does not care at all about markets of that size. Unless there are 100 million or so sales involved, they are not interested. The globalization of IT has simply taken banking off the radar as far as key technology providers are concerned.

As far as the telcos are concerned, their main battle is to avoid being held liable for the content that flows over their networks. They want to maintain the mere-conduit defense against all sorts of possible lawsuits over everything from peer-to-peer systems to pornography. They would resist very, very fiercely an attempt to put regulatory burden on them.

The way it is seen by folks in places like Microsoft is this. Twenty years ago, when you offered someone an electronic banking service, you shipped them their own software. You shipped out floppy disks, CDs, or whatever to people who had such systems. The banking industry—the view of Microsoft is—is essentially free riding off this commodity technology that has been made available to everybody.

If the banking industry wanted to tighten up security, then banks could issue their customers with client software rather than having them use commodity browsers. Yes, there is a good point there, Cathy, but the problem is the economics have moved against it at the supplier side. At the bank side, do you want to be the only bank in your state that is spending several million dollars a year maintaining your own custom client software?

Mr. Van Dyke:

Just briefly. I believe—and this is the ideal forum for a subject like this—regulatory questions must be talked about within the same

context of self-regulatory issues and branding issues. All three work together. They play a very complementary role—regulatory, self-regulatory, and branding. Sometimes, as with any set of tools, they have a unique role to play. One might be better than the other. That is why they all three must be considered together. In particular, regulatory efforts are more likely to have more effectiveness and be more appropriate where you have nonfinancial providers being account custodians in ways that are most akin to what banks and traditional payments firms do.

Mr. Michael Cook, Vice President and Assistant Treasurer, Wal-Mart Stores, Inc.:

Do you have any statistics on how many banks—or even the four card networks—are PCI-compliant themselves? (The question is probably for Jean. There are two parts to it.) The second part of that question is, If the PCI guidelines are such that only the last four digits of the card account number can be printed on a receipt, is there a reason that banks are allowed to print the last 10 digits on convenience checks on both the front of the check and in the MICR line—banks such as HSBC, Capital One, even Chase Bank?

Ms. Jean Bruesewitz, Senior Vice President, Visa U.S.A.:

Well, thank you. We do have the records on PCI compliance, and we can certainly share them with you and would have Mike Smith, who runs that risk area, contact you. So, I will be glad to do that.

Mr. Cook:

We have asked that question before on how many banks are PCI-compliant, and we have been told that you don't know yet, and we have also been told, at a separate time, that you can't give out that information.

Ms. Bruesewitz:

I will have him contact you directly.

Ms. Litan:

In terms of the check information, I do not know who can answer that. Maybe Rich can.

Mr. Richard Oliver, Executive Vice President, Federal Reserve Bank of Atlanta:

I don't know the subject.

Ms. Litan:

One of the issues I have seen in the check area—at least we have PCI to pick on—and the ACH area is there is really no set of

comparable rules about what you can print. Good, I am going to be corrected.

Mr. Oliver:

No, I think that is exactly right. I think you have a very practical issue here of clearing the payment. You need to have information that is sufficient on the document to clear the payment back to the proper account. That is a big distinction between these types of services where you are using an instrument in the clear. It is a nuance of the system that is particularly difficult. Mike has a question.

Mr. Cook:

I want to follow up on that. I would want to recognize, though, that Citibank and American Express do not use the account number in the MICR line. They tie it to a different number.

Mr. Oliver:

There are growing ways to disguise that. In the ACH environment, the clearinghouse has been working with something called UPIC, which is an attempt to try to give corporations an opportunity to not reveal in the front end of their transaction their corporate account numbers and map them back later through a database.

Things like that may need to evolve in the environment, but I go back to the same thing Professor Anderson said, it is this horrible confrontation between the economics of what you are doing and the protection you think you are going to get.

Ms. Litan:

But then it also comes down to what your paper said about who bears the liability because now a lot of the liability shifted from the parties that can control the risk.

Any other questions? Yes, Steve.

Mr. Steve Mott, Principal, BetterBuyDesign:

I am Steve Mott from the payments systems consultancy BetterBuyDesign with a "buy." I would like to say for the record that most of the research, including Edgar Dunn's on fraud, shows that financial institutions do a heck of a good job on management of fraud overall, particularly compared with health-care and insurance industries.

That said, a lot of the emphasis right now seems to be on transaction monitoring and identity management, while the transaction is en route and the security that is involved en route. I think one of the most interesting things about Professor McDonald's treatise here is looking at the pain points at the endpoint of this transaction flow, but I

would also think at the front end as well. There is a lot of scrutiny now occurring in Washington about is it too easy to come in the front door and set up an account once you compromise, in the United States, a Social Security number and thoughts about changing that as a means of requirement.

You think about nonbank participation. When PayPal sets up a DDA account, they have this patented mechanism where they post two ACH transactions totaling $1, and you have to report back that you have gotten those two right in the right amounts in order to set up that account for use. It seems like a pretty good mechanism, and a lot of people think that is better than a lot of financial institutions' practice today for an account setup, particularly online.

At the back end, where a lot of the pain is, once you are compromised and the crook pushes you out the backdoor, trying to get back in is almost impossible. It takes months and years. That is true even with a nonbank like PayPal. Once the breach has occurred in the account, the legitimate accountholder has a bad time trying to fix things. It takes a lot of time and a lot of effort. Jim did a lot of research on that.

My question to the panel is, Is it too easy to set up an account and to take over an account? Is it too hard to fix it? And are we addressing that as an industry sufficiently?

Ms. Litan:

Well, I will take the beginning of that. I tried to mention that with the DMV Real ID Act that the source documents are easy to forge, so we need to get that right. In my opinion, identity scoring is a much better system than black-and-white identity verification against known documents or known data. In other words, we should not rely on a Social Security number, a date of birth, a name, etc. We should look at all the characteristics of that identity, just like credit card fraud scoring does with its own neural networks.

We look at the identity behavior, and, if we are sharing data across industries and sectors, it is even better because we can look at how that identity was behaving in the last few months or years. Of course, there are major privacy implications with this type of system, but my own personal belief is we should not rely on driver's licenses and Social Security numbers. We should rely on a score. Anyone else want to answer this?

Mr. Roy DeCicco, Senior Vice President, JPMorgan Chase:

If I could just add to that. In my remarks, I was talking about some of the industry data that are out there—companies like Early Warning Services—providing tons of information on consumers, on DDAs, on fraudsters, on closed accounts, so on and so forth. As we continue to get more sophisticated as an industry in collecting those data and

sorting through it, we could tap into that as we get customers coming to our front office or through the Internet and opening accounts. We would be checking against those data files to confirm the identity and the history of who they are as we put more and more of that information together.

Mr. Van Dyke:

If I could comment on the neural net concept that you mentioned, what I think is really interesting is fundamentally what a neural net does is mimic the way the accountholder thinks or operates and yet we are leaving that accountholder business or consumer out of the equation. Why not just authenticate the accountholder or applicant better, and then harness the identity-holder's motivation to join the industry in fighting criminals?

With user-defined limits and prohibitions (UDLAPS), why not let the accountholder tell us in advance under the most strongly authenticated session, not just three-factor but four-factor, with mobile technologies or even IP-based technologies indicating "where you are"? Let the user define the parameters under which account transactions should be allowed and then use emerging technology for more effective notification.

To answer the beginning part of your question, we clearly see that overall the number of hours of resolution for the typical user is dropping year over year.

Mr. Anderson:

There is perhaps an interesting European perspective in this because first the security economics community decided a few years ago that identity fraud is not, in fact, that. It is, for most purposes, libel, at least from the point of view of the customers. If you go through Barclays bank, pretend to be me, borrow £10,000, do a runner, how can it not be my problem? That is impersonation. That is a crime committed against Barclays.

The problem we have nowadays is that this gets rebadged as identity fraud, so it is not Barclays money that has been stolen, it is my identity. Now hang on! I am not a party to this transaction. If I were able to sue for libel, then I could stop the credit reference agencies' retailing untruths about me.

What can actually be done? Well, the interesting thing is in Britain we have Section 1 of a Debtor Protection Act, which makes it an offense for people to knowingly hold and disseminate false information about debtor subjects. And there is now some pressure coming on to our information commissioner, who regulates privacy law, to start enforcing this against the credit reference agencies. If he

starts doing that, then recovery from many kinds of identity fraud will become very much simpler and less painful from the point of view of the debtor subjects.

How that would run in America, which does not have privacy laws, I do not know. Perhaps there is some scope for some regulator, whether it is the Federal Reserve or the FTC or whatever, to lean on the credit reference agencies and say, "Thou shalt not bear false witness against people who are actually known to be simply the innocent victims of identity fraud."

There is definitely some scope for action there.

Ms. Litan:

Just a simple anecdote, though. The IRS will accept tax returns with duplicate Social Security numbers, so there is no one responsible for that. The credit reporting agencies will say, "We are just taking what we get from the source agencies."

The IRS will say, "We don't really know who the rightful owner of the SSN is."

It is an accountability issue.

Ms. Bruesewitz:

I'd like to add from a Visa U.S.A. perspective. If we look at all the card fraud that exists, the actual new-account fraud and account-

takeover fraud are running 10 percent to 12 percent. That is a lot different—having your card number stolen, having your card number in a database, getting that shut down, and getting a new card number issued is one thing. When your personal information is out there, which is really identity theft, it is very difficult for consumers. They have to recover their credit reports, as you all know. That is the tough part. Managing through the fraud side from a card perspective is actually a pretty quick process, but it is the real identity theft that is of concern.

Ms. Litan:

Any other questions?

Mr. John Muller, Vice President, PayPal, Inc.:

Hi. John Muller from PayPal. I have a question on the issue of not putting the financial burden on the consumer for Avivah. In your research that showed that the rate went down from 60 percent recoveries for consumers to 54 percent, did you get data on how to parcel out among consumers who did not try to recover because the amount was small versus consumers who were using non-Regulation E-covered systems versus banks and nonbanks that try to use an exception to Regulation E to deny their recovery?

Ms. Litan:

I would have liked to, but we try to keep the questions answerable and kind of short. What we did ask is, Where do you think you lost money? If you did, what was the brand that was being impersonated? Then, we asked, "Did you try to recover your money?" So, I have data on that. From where did you recover your money?

An interesting trend is banks and credit card companies are going down as the source of where consumers are recovering their money from and also as the brand being attacked. It is all these unconventional attacks that are increasing. It is harder for people to get their money back as a result. Those are pretty much the data we have.

That's time. Thank you very much for coming to the panel.