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: James Van Dyke, President, Javelin Strategy and Research

Mr. Van Dyke: [remarks correspond with handout]

Thanks, Avivah. It is hard to know where exactly to jump in on a very stimulating panel when coming up at the end of the alphabetical order here. I took my last-minute notes and added so many last-minute notes to my last-minute notes. I will try to make good use of the time, stay organized, and not sound like I have taken an Evelyn Wood speed talking course here.

As quick background, I have 23 years in electronic commerce and launched online banking, encryption systems, a lot of product management, with a lot of research, a lot of background in electronic commerce in the early days and early pre-Web stuff. What I am seeing is we are going to frictionless commerce. We are also going to frictionless fraud. And yet, the long story short, if I were to sum up everything I am about to say, would be in order to beat this frictionless fraud trend, we need to get to frictionless partners across the industry and also with the accountholder. Stop treating the identity-holder as someone who essentially has a first-grade intellect and add value, but

rather realize they want to and can play a vital role. Given that, if they are not being effective, it is our fault for not properly enabling them.

We also need to tie in the back end with the front end—within everybody who is an account provider, whether that is a nonbank or a bank, and everybody else who holds or influences an account provider relationship.

A couple of comments about how I perceive this topic. Among three interrelated areas on which we do research—payments, multichanneled financial services, and risk/fraud—we are very much in the customer-facing side in our research, and we do back-end work, as it affects the customer relationship. Our focus is a little bit different, as Gartner tends to focus a little more on the back end, with extremely strong IT successes over the years. What we see on that is that, within the area of identity fraud, it encompasses just a third of our research but 90 percent of all the misunderstandings we see. So, it is important to look at research. Each of us needs to arm ourselves with rigorous, nationally representative and current research and ask ourselves, "Where are the misunderstandings, and to what degree are they significant in influencing policy decisions I'm working on right now?"

I said there are five major bodies of research that drive what I am going to talk about. One is, since the first few months we were

founded five years ago, we started polling people on an annual basis through an online survey to check behaviors and attitudes.

We also do the largest poll by telephone on the planet of ID fraud victims, and it is now up to 19,000 people. It is longitudinal to the Federal Trade Commission 2003 study that originally broke a lot of the news that we are still thinking in terms of about risk and payments. We also do a mystery shop survey of every major US issuer and bank in the industry. Today it represents 60 percent of the actual account relationships—great institutions like JPMorgan Chase, credit unions, and others. We built up looking at victim data and attitude and behavioral data, we say what is possible, what features banks should have that face the customers, and then we score those institutions on the features and revise it every year. In fact, we are just wrapping polling of the top 25 US issuers right now.

We also completed in-depth interviews of 60 global CISOs—North America, India, South Africa, Western Europe, and other areas—and various other custom studies.

What we are finding is this dramatic pattern of misunderstanding that we really only see within the area of identity fraud. We are not seeing these big disconnects in our payments research and multichannel financial services research.

To give you a quick credibility test, five years ago, I arrived at what we call the “null hypothesis” in research. I suspected that most of

the risk in online shopping patterns could be avoided through certain readily available consumer practices, but I found that not to be the case. Yet the research turned up significant opportunities to mitigate fraud through electronic (paperless) deposit account management and monitoring. There is much we can do with the accountholder; we can do a lot in deposit or ACH relationships, and certainly checks and other areas. This is where the misunderstanding is so great: Much of the power to protect the individual actually rests in cooperative and electronic efforts of working with the actual holder of the account and identity. So, my belief that I started out with actually shifted when I looked at the data.

Most people believe that most fraud occurs with data breaches and Internet usage. You ask consumers or you ask many industry executives, hands down they would tell you this is the case. If you give them a list of possible actual causes of transaction fraud—not potential threats—they would always pick out those two. You add those two—and you especially focus on phishing and data breaches—based on victims who know how the cause of their fraud occurred, 7 percent of all known-cause losses. You cannot get to a model that reliably would tell you, even if you assume that everybody who did not know the cause of their losses was a victim of data breaches and the Internet—even in such wild modeling, you cannot get to a model that says more than half of all fraud is made possible by

accountholders being online, even if you assume that everybody who did not know the cause of their loss was a victim of electronic crimes.

If we are setting policy on the belief that most crimes are occurring due to individuals' use of electronic services, we are in trouble because we are out of step with the facts. There is this belief that institutions' most effective efforts are in fraud prevention. Rich talked about prevention detection and what we call "resolution." Our scorecard tells us the most effective efforts in the banks and other providers, even nonbanks, have been under resolution not prevention as we score out this.

Just like with Katrina, you have to pluck the victims from the housetops when there is a flood before you can put all the resources on stopping the dike that is letting the water come in. That is something you have to do. You have to treat the victims first, and indeed, that is what the industry has done.

People believe that accountholders have little to offer to actually mitigate fraud in a material way. One in two actual fraud causes year in and year out, based on 100 percent of victims—and I have been an ID fraud victim four times (we do throw out a lot of the responses we get when we do not deem them to be reliable)—are first detected by the accountholder. They can play a significant role.

There is also this belief that accountholders do not want to be involved in security, when nothing could be further from the truth

when you look at the data. Not only do they want to be involved, they will migrate to providers that make it easy. If it is not easy, it is our fault for taking someone who just wants something to be simple.

Example of that: Most bank websites, until a few years ago, when they talked about Internet and security, would only tell you what could go wrong. They did not tell you how you could use this emerging channel to help make things go right—that is, better—across channels and security. (I can explain more on that if it is confusing on a break; just watching the time here.)

There is this belief that most ID fraud crimes are committed by distant perpetrators. Certainly, you will get more online fraud attempts, but we cannot confuse attempts—which would be greater in number—with actual fraud cases. Much known-cause fraud is carried out by those close to the victim.

Just think about the knowledge-based authentication (KBA) methods. There are 10 people I could defraud today because I know enough about them to provide their mother's maiden name, previous places they had a mortgage, and information like that.

There is a belief that the elderly are typical of most victims. It is absolutely not true. There is a cause-and-effect relationship with young people. Surprisingly, younger people who grow up around computers are actually doing online banking without having protection on their computer. They are throwing full financial statements in the

trash can and receiving them through the US mail. Isn't it bizarre that we wisely demand SSL to encrypt online data, but we do not think it is a dangerous idea to send account numbers through the mail? We need to think multichannel, just as criminals do.

There is also this belief put forth from a Cal-Berkeley lawyer who believes that leading banks, such as those in this room, are in conspiracy to hide a problem of growing identity fraud, which is growing by leaps and bounds due to the Internet and data breaches, and that we are the research firm enabling you to hide this problem through our research. That is a true belief that a very small number of people have been repeating, and yet no credible source of data supports that. ID fraud has leveled off, and if you looked inside the data, you would be surprised how much data we did not publish that really bolsters that. I predict that we will see it go down further even next year in the US, but it remains a very difficult, $48 billion problem for the industry and victims.

One last misconception is that electronic channels are actually lowering individuals'—business or consumer—usage of the Internet. In fact, fear of fraud is making people's logins go up by an 8-to-1 ratio because people at some level know their best defense against fraud is to monitor their accounts more frequently. So, surprisingly, they go to the channel that allows them to log in more. Mobile banking will be much more secure than the Internet for a variety of reasons, including

frequency of interaction and variety of platforms. Yet we need to be careful, to use another adage, that when you have a hammer in your hand—that is, you feel you have this control in fighting phishing attacks and data breaches, which we need to be all over—you tend to treat everything like a nail.

Just to close on a quick, short laundry list of topics, we need more self-regulation. For example, when Visa and MasterCard effectively shut down CardSystems, that was good, healthy self-regulation. We need to watch accounts like e-gold. We had somebody impersonate Javelin last year and try to make phishing victims of banks using e-gold. That was one of my four personal cases I've been involved in.

We need to watch out with data breach notifications. I am a big fan of effective consumer notifications, but more is not always better. After a while, people lose count. Most of you probably do not remember, but when you were on aircraft coming out, you might have been told that if you disabled the smoke detector in the aircraft, you were breaking a federal law. You probably do not remember that because you tuned it out long ago. More data breach notifications can be good, but they also create a white-noise factor that deprives individuals of vital information if we are indiscriminant with them.

That brings me to the quick subject of brand. When you look at a couple of security-based payment launches that were successful, so to

speak, it causes us to want to raise the question of, Should we be branding more in things like PCI? I will raise it as a question.

Here are two examples. Example 1: American Express Blue. It is 1999, we are on the verge of the height of the dot-com era. It was a highly successful launch by all outward accounts. From a marketing perspective, it was based purely on security, and most of us who observed this knew that the consumer was not one iota safer. The chip did not do anything—physical point of sale, online, the devices were not set up to work. The POS devices were not set up to read what was on the chip, and yet Javelin believes that it drove consumer selection and loyalty behavior.

Example 2: Online bank selection. FDIC branding in our survey data still steers consumer behavior. Guess what? Every depository institution has FDIC backing of your funds. The point is, can we drive more compliance by elevating the brand that shows who is keeping the accountholder safe? It is really a healthy corollary conversation I had yesterday about surcharges, trying to figure out where the incentive is.

As we studied TJX, an interesting thing was that consumers said, "I will not shop at a merchant where my information is violated." And yet TJX just posted record profits. Because there are numerous questions about how to best prevent, detect, and resolve fraud, they are vital; difficult; and very, very complex stuff. I will close by saying we need to tie the back end with the front end. Even though I said that I

believe new technology channels are often myopically viewed as having only downside, not upside, and we view that at our peril, I will say that nonbank payment or financial methods often do introduce more real risk, as opposed to the new technologies. So, I do not want to confuse new technology with alternative financial services and payments methods where I do believe there is more significant risk.

That concludes my comments.

Ms. Litan:

Thank you, Jim. Just one comment on the data. In the United States, there is no official mandate for financial institutions or anyone else to report fraud data. I think there is in the UK, isn't there? Banks in the UK have to report their fraud data.

Mr. Ross Anderson, Professor, Cambridge University:

Yes. APACS is reckoned to have fairly reliable fraud data.

Ms. Litan:

That is another point. Now that I have an audience of regulators, I would like to make an argument that we should get some data from the financial institutions because they are in the best position to give reliable data.

I want to open it up for audience questions.