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: Roy DeCicco, Senior Vice President, JPMorgan Chase

Mr. DeCicco: [remarks correspond with handout]

Good morning, everyone. I am going to take a banking industry perspective on e-payments—what JPMorgan Chase is doing and what we believe the industry is doing more broadly around securing electronic payments, both at the retail and the wholesale level. In front of you, you have the remarks I wrote for the conference, so I am not going to read it, but I will paraphrase and go through some of the highlighted points here.

Professor Anderson spoke about recoverability and revocability of fraudulent payments, and that really time is of the essence when you find a fraudulent situation. From our perspective in the industry, I think we would agree 100 percent that speed is important, action must be taken immediately once the facts are known, and most institutions have what I am calling a "fraud and protection infrastructure" that allows them to create an aggressive recovery plan when fraud is perpetrated.

This infrastructure includes loss-recovery specialists. We have loss-recovery specialists both in the wholesale business and the retail

business. They network internally with the legal, security, and payments subject matter experts in any given situation. When necessary, they will reach out and speak with law enforcement officials and with other banks that may be involved if some of their information has been placed in jeopardy.

So, this process exists today. As Professor Anderson cited in some of his statistics, the banks that are good at this will be able to recover far more than those that do not have that ingrained in their culture or do not have a good fraud and protection infrastructure.

What is equally important to us in the industry, however, is fraud mitigation at the front end of the payments cycle, reducing the likelihood that fraudulent transactions will ever occur. Again, to borrow a theme from Professor Anderson's paper, our objective is to strengthen the safety and soundness of our payments infrastructure, so there is little or no economic incentive for the fraudsters to attack that channel. If there are better channels to attack because they have a better probability of making away with the funds that they are looking for, they will go there and they will avoid these types of channels.

This is a multifaceted scenario. There are a lot of different parts to this. There are a lot of different players in it, both internally in our own organizations and extending that process to other players, very often including our own customers.

When you think of what is happening now, for example, in our industry with back-office conversion—I was with Rich Oliver at a Fed conference in Atlanta last fall and one of the things we talked about was back-office conversion. What back-office conversion will be doing in the industry, which now allows—for those of you who are not aware of it—merchants to accept the check payment, but instead of converting it at the point of sale, at the cash register, and giving back the check to the customer and electronifying the transaction at the cash register, they will not change that customer experience. They will complete the transaction as a check transaction, take all those checks in the back office, and go through a conversion process in the back office—so, a not-so-subtle difference in trying to electronify the check, but a major difference in terms of data storage and security. Now merchants will have thousands and thousands and tens of thousands of checks they have accepted, they are converting, and they need to retain for a period of time. How do they retain those checks? So, that is a standard we need to continue to get out to our customers, to educate them on standards around that and to ensure that is being secured properly.

Customer vigilance. Consumers and corporate entities are key players in our payment channels. Their knowledge, their awareness, and their vigilance will help ensure security over their accounts and over the payments systems they access. Clearly, if they are not at the

top of their game here and they fall victim to a phishing attack, as an example, even the best-secured payments system in the world is not going to help. So, there are some basic things we think customers need to do. They are pretty basic things. They have been out there, but again, education is important. Education updates on what is happening in the marketplace to our retail customers and to our corporate customers are critical so they stay on top of the latest developments.

Many banks have websites. We have one, AbuseAtChase.com, where clients can come in and report on suspicious e-mails or on suspicious phishing attacks that have to do with our name. We want that information, and we will follow up on it very quickly to ensure we can close any potential danger there.

The role of industry organizations. BITS and NACHA are two of many that are playing an important role in examining safety and soundness across payments channels. The BITS Partner Group, which is an industry group of financial institutions and corporate and government subject-matter experts, has examined cross-channel payment risk, focused on very specific items, such as promoting data sharing, closing liability gaps, and developing standards for third-party access to payments systems. So, there is a lot of good work in that regard and there will be action in terms of takeup on some of the recommendations that The Partner Group has developed.

NACHA has a comprehensive risk management strategy meant to ensure high quality in the ACH network. We think the ACH network has good quality. It has done a lot to bring down the rate of unauthorized transactions, but you have to keep vigilant—never-ending vigilance. There is more that NACHA is doing, and I believe Rich is going to touch on some of the details around what the NACHA community is doing.

In my remaining time, I would like to focus on three aspects of what bank payment service providers are doing to promote safety and soundness: protecting clients' electronic credentials, protecting clients' electronic transactions, and empowering clients to manage user and access controls. You have heard a lot about multifactor authentication—how secure it is and how prone it is to further attacks by the fraudsters. They are strong security measures. If as an industry we need to make them stronger, we need to continue to do that.

Two-factor authentication is good; three factor is better, particularly as we start to look at the aspect of including something you are, such as a retina scan or a fingerprint, which we will see more takeup on as they become more commercially warranted. And then basics in terms of protecting electronic credentials, securing your passwords, strong password guidelines, so on and so forth, need to continue to be reinforced.

Protecting high-risk electronic transactions. Something that some providers are now doing is requiring a digital signature as a second level of authentication before payments are released to the bank for processing. In the course of researching this, the security people gave me an interesting term I was unaware of: time decay of trust. That principle is that the longer the time from logon to release of a transaction, the less comfortable the bank is in processing that transaction. What banks are starting to do is say, "Listen, it has been a while since you created this transaction. We want a second authentication to, in effect, reauthenticate that transaction."

Banks are also developing capabilities to check clients' payment instructions against industry databases before finalizing payments. This integration of information and technology will be useful in fighting fraud because it is providing banks with current and accurate account-level information in making a payment decision. Going against those databases, banks will kick out transactions for payments, where the debit party account is subject to fraud or perhaps has been closed already and the industry information knows it.

Finally, empowering clients to manage user and access controls. Sarbanes-Oxley is placing a higher emphasis on this, and a lot of corporate cash managers and treasurers are now on the same page as their bankers in saying, "I need to control my user community. Give

me the right tools through the access systems I use from you as a bank provider to do that, and I will manage it carefully and aggressively."

These are some of the things that we are doing. We need to continue to work together because we are constantly at risk. The attackers change. Their methods change all the time. I would agree with some of the comments that have been made around transparency, around responsibility for protecting data. If you have data, you have to have responsibility for protecting it because if you do not protect, then you should be responsible and liable for some of the ultimate outcomes of that. That philosophy is becoming more and more ingrained in our industry. That is a step in the right direction. Working together, I think we can continue to help protect each other. Thank you.

Ms. Litan:

So, when you look at the landscape of your own bank, what do you see as the main vulnerabilities? Where are you most concerned?

Mr. DeCicco:

I am concerned where we do not have control over the data and where our customers, as you extend the payment chain through automation and technology, what we are doing is empowering a lot of our customers to provide some of that input. As they provide that

input, they have responsibility for managing some of those data. I go back to that back-office conversion example I used. One of my concerns would be, How are clients managing control of the data they have in their possession after they have used some of the new technologies and electronified transactions?

Ms. Litan:

You raise a really good point, and you also talked about the need for a standard similar to the PCI standard on the card area. Where do you think that standard should come out of, and who would manage that?

Mr. DeCicco:

I hope it comes out of the industry. We have two choices around that. We can go to regulators and say, "Help us and regulate it!" But that is not the way we in the United States prefer to do things. When we talked about it at the conference in Atlanta in October, there was a fair amount of acknowledgement and concern over the issue. My takeaway from that was that we would be looking for the industry to lead that and take some steps to create standards and to educate our extended custodians of the information on what those standards are.

Ms. Litan:

My problem is I am not a big believer in customer education. On my own, I am a consumer and pretty well educated about the threats out there. But I cannot keep up with all the vulnerabilities, and I am glad Gartner manages my PC for me. I do hear a lot of companies are putting emphasis on customer education, which sounds like the right thing to do, but is it really effective?

I looked at my own survey results on phishing. There has been tremendous education on phishing. A lot of consumers still do not know what it is. When I asked about their awareness of phishing, it was way below viruses because Norton has been out there selling virus protection. So, can you talk about the practicality of not only consumer education, but also these retailers that are going to be storing check data. Education is not an easy thing to rely on.

Mr. DeCicco:

No, it is not. It is a necessary first step, but anybody who is a provider in the payments industry cannot just say, "I have done my due diligence, I have educated my customer, I am going back to give them a refresher every six or 12 months, and my obligations are completed."

The industry has to take a next step and go further than that. It is all part of KYC—know your customer—know their business, know what transactions they are doing with you, know what the risk aspects

of those transactions are. And if part of the risk aspects—again I will use back-office conversion as an example—they are one of your major clients in using that particular service, you want to ask some more detailed questions. What are you doing? What is your security? Here are the standards. Here are the best practices. Are you compliant with that? You have to get that confirmation back from your customer.

Ms. Litan:

It reminds me—I was reading an article last night about diversity in organizations and how companies actually moved to hire a diverse workforce. With training, it did not get anywhere. It did not get anywhere until they made someone accountable for implementing diversity. It strikes me as the same thing here. We are pushing all these data out to consumers and to businesses. We are trying to say, "Okay, we are training them. They should be responsible." But there needs to be accountability

Going back to the question on accountability, Professor Anderson talked about recovery of funds. Let's say a consumer falls for a scam—for example, a Nigerian scam. I do not mean to single out Nigeria, but they seem to have a lot of scams. It is not really the bank's responsibility, is it? If someone falls for a scam, how are they getting their money back? Have you thought about a mechanism that

could protect consumers? What is your thought on that? I know that is a difficult question.

Mr. DeCicco:

It is a hard question. How do you foolproof the system? I do not know if you can ever foolproof the system. I really do not think you can. You can tighten it. You can control it. When your retail client falls for one of those scams, reports it, and the fraud was run through their account with you, you can take whatever appropriate or best steps are there to help try to recover the funds. Now you have an educated consumer, I guess, but not the way you wanted to educate them. I do not know if you could ever foolproof the system. You can just keep the notices out, keep the alerts out, and help with recovery when that particular scenario happens.

Ms. Litan:

So, one last question. We talk a lot about consumer protections. You are from treasury services, it seems like business banking customers do not get the same kind of attention consumers get. For example, in terms of revocability, they have two days to report a loss under Regulation E versus 60 days that consumers have. Can you talk about the risks of business banking, and what you are doing there relative to consumer banking?

Mr. DeCicco:

Business banking customers, for the most part (there are always exceptions to that rule), are more sophisticated and more aware of their responsibilities in using the payment channels. They have all of the security tools we develop as an industry. We continue to educate them. They do not have Regulation E 60-day revocability, but when they have a fraudulent transaction going through their account, we will use the same recovery aspects. It is a different team than the retail team, but the wholesale team will spring into action and will use all available means to go back and recover their funds.

Ms. Litan:

Are you seeing more risk in the consumer channel or in the business channel? Where is the fraud showing up?

Mr. DeCicco:

Actually, it shows up on both channels. I talk to the recovery people on both sides, and their to-do lists are both long. It is in both channels.

Ms. Litan:

Okay, thanks. We will open up to audience discussion once we get through the panelists. Thank you. Rich, you are next.