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

Mr. Oliver: [remarks correspond with handout]

At this point in the panel, after you hear all this, there is a tendency to react in despair to the challenge ahead. And, after everything you have heard, there is also a tendency to wonder what you are going to say because so much has already been said. Let me take a shot at this from the angle of a practitioner and intermediary in the payments system, which is the unique role we have here.

I have to tell you, in taking over the retail payments environment in the Fed of checks and ACH, one of the things I really had to come face to face with early on was the difficulty of trying to manage a payments business in this era of fraud and security issues and to come face to face with the fact that, first off, I have to view the whole issue as a business management issue. You have to go about deciding what you are going to do here as a business proposition.

You look at investments. Where do you spend your time? Where do you get your biggest bang for the buck? Ultimately, that is part of what we are all confronted with today. Where do I get my biggest

bang for the buck? As Professor Anderson was saying, it is probably not with identification anymore.

Having said that, there is another element to this particular problem, and that is the reputational risk that goes along with it. The problem gets bigger than the finances, and it forces you to consider options that you probably have not considered before.

It also occurs to me that, if you take the process of managing fraud and security and divide it up into three components—let's say prevention, detection, and response—that it is an ever-escalating game. Wherever the weak spot is, is where bad people flow. In essence, that happens and it happens across channels. You find yourselves in an interesting game today, where various payments systems are competing on who will be the least vulnerable, hoping for the activity to move someplace else in the meantime.

It reminds you of the old joke about the two guys being chased by the bear. One guy says, "How are we going to outrun the bear?" The other guy says, "I only have to outrun you."

That is pretty much what is going on in the payments system today. You have to try to make your piece of it the place where people do not want to go. As an illustration of that, a few weeks ago, the Payments System Policy Committee of the Federal Reserve, chaired by Vice Chair Don Kohn, put on a fraud roundtable in Minneapolis. We had about 15-20 individuals, key players from all aspects of the

industry. We talked about this, and there was widespread agreement that 80 percent of the fraud occurring in U.S. retail payments today is occurring in checks because they have become the place that is easiest and where the water is flowing.

Now, when you look at that, you ask yourselves an interesting question: Are there any of us in the room likely to spend a lot more money on investing in check fraud when you have a system that is in major decline and the losses tend to be relatively modest. Probably not—but, because things operate across channels, it does signal that we have to pay attention to that particular type of assessment. That is why I came to the conclusion it requires a comprehensive attack along all fronts.

Not to dispute the professor's comment that perhaps we have run course on identification, but I certainly know that, within the ACH environment, that is not true. We have not done nearly enough on identification at this point in time to seriously address fraud, really ascertain it. Look at online purchasing. Have they done enough on e-tailer sites? Probably not. So, there is much more work to be done there, but that does not mean we should not concentrate across the board. I agree with Avivah that a comprehensive approach is the best.

Looking at that, I want to use ACH as an example. Roy and I serve on the NACHA board. I want to use the ACH to amplify a couple points and look at the identification process. We have had an

ACH network in place in which the originator of a payment, the company originating the payment, is not even required to put a valid telephone number or company identification in the record. That, then, goes over to the professor's point that if you don't have that, how can you ever trace the item; how can you ever find the payments? That is an issue we have to get at, and in fact, there are rules being put in place today to try to strengthen that.

If you look at detection, there is a lot of work going into the issue of detection now, trying to understand what is happening out there, where the problems are, and then getting to them quickly by looking at unauthorized return reports and a variety of other things. But going back to the earlier comment that speed and aggression are important here in this issue, we are looking at ways to rapidly expedite processes that are going on and problems that are evolving in a way that can stop them as quickly as possible.

But also you can look at them more systematically. We have a group of folks in the Atlanta Fed who have developed a risk model that takes a look at the practices of all institutions that are classed into peer groups. What they do is they look at their typical behavior of ACH debit origination against capital and assets. They profile what is typical for the group and look for outliers. They use the outliers as indications of what they should do when they go into that bank. There is a particular point here they need to focus on in asking the bank,

"What are your risk procedures, and how are you controlling your exposure?"

Counseling, action, fines, and response, all those things are important, and I want to settle for just a second on the issue of punitive damages. It is clear to us in managing the business, if you want people to pay attention, raise the price on violations. Make it worth their while. So there is a system of fines and penalties going in to get at institutions who do not respond effectively to all of the counseling and direct action that come from trying to detect problems, and they will have to step up because they *are* in the best position to stop it and make it happen by doing a better job with their customers.

You have to move then to regulation. We do have, fortunately, a user-friendly Regulation E in this country, as the professor said. It is a big boon in how to settle disputes. But, by the same token, there are more regulations that need to go in place.

In addition, we have the supervision issue here. Supervision is not just about bank regulators; it is about SEC and the FTC, as well as all the banking regulators. And I want to finish on something on that point. When you take all this and throw it into the nonbank environment, you come face to face with a serious business proposition that banks seem to have today. That is, that the nonbanks have been particularly effective and entrepreneurial in developing niche payment solutions that use technology properly. We folks in

banking have not been the best users of technology on Earth, we are not the smartest people when it comes to that, and we are not as innovative. So, now we find a time where banks actually want to use third parties to do part of their business, particularly as profit margins fall. With that in mind, responsibility begins to focus then on banks to know their customer and know their customer's customers—which is a new part of the game—and be responsible for the actions they take in utilizing third parties.

The regulators, on the other hand, have not done a good job of integration. We have to do a better job and get the banking regulators and the other two I mentioned—the financial institutions and the big industry bodies like NACHA, BITS, and others—together in a room and say, "What is the best comprehensive way to make it work?" Frankly, there are silos between the regulators. They do not easily step forward and cooperate with each other, but if they did, it would be a huge step forward.

In closing, I would simply make the point that it does not matter what we do or where we focus if we do not do it on an integrated basis because the bad guys will move to the place that is the weakest. We need a comprehensive, cross-channel, cross-regulator, cross-industry assessment of this to be truly effective.

Ms. Litan:

That is totally true, but how achievable is that?

Mr. Oliver:

It is going to be really hard. It is pick-and-shovel work. The only thing that makes it possible in my mind is I hear more people willing to talk about it. The BITS' efforts have gotten people to the table who have not previously been willing to talk with each other—card companies and so forth—about their techniques and approaches.

I know the regulators are spending more and more time on this issue. In the last year, we have had the FTC shut down a banking operation. We have had the SEC shut down a company that was causing fraudulent behavior through a small bank. And we have had banking regulators getting more involved. There are regulators right now in two financial institutions that have been dealing with recurring fraudsters and have been slow to respond. That is an example of how regulators can act more expediently than they do today, rather than every two years. There is a willingness now to talk about these things. If that is there because it is an increasing problem, hopefully there will be a willingness to come to the table.

Ms. Litan:

Can you be a little more specific about where you see the need for integrated regulation? What kind of fraud are you seeing out there where that would apply, and what would it look like?

Mr. Oliver:

Certainly on the identification front, when you find a bad player in a card network or the ACH network, to more openly share that information with the other networks that these same bad players may be doing business through. There was a case involving a company in California called 12 Daily Pro that made the news last year. It was a Ponzi scheme investment case that was preying on individual investors.

All the discussion that came out then was about what happened on the ACH side and all of the unauthorized returns that were coming back to this small bank—$750,000 a day during the peak—to a very small bank capitalized at $20 million. What was not said was there was just as much card fraud that had gone on with that situation. Yet, the two networks had no idea the same business was in action.

Ms. Litan:

We found that in our own research on fraud-detection systems. It really helps when companies and sectors share information because

the bad guys just don't attack one channel, as you said. You can usually spot them through a common identity or a common IP address.

Can you talk about the nonbank payment providers? You talked a bit about that, but could you elaborate if they have introduced new risk into the system?

Mr. Oliver:

Well, they come in two forms. Every time I have a conversation on this, we have to talk carefully about what we mean. There are plenty of nonbank payment providers out there today that include bank service bureaus, as well as large reputable organizations—like CheckFree, ADP, and others like that—that are totally ingrained in the payments system and have been given access to the payments system in essence by their banks. We have a lot of that going on with the way that a lot of the remote-capture stuff happens today with access.

Having said that, there is clearly another element of nonbank entities. Whether they are payments providers or what, I do not know. There are certainly people out there who want to go to financial institutions and convince them it is in their best interest, and perhaps their best financial interest, by giving them part of a fee structure or something like that, to allow them to have a greater role and responsibility in managing payments that go through that financial institution's accounts. I think that is the place we have to focus. We

have to focus on the people who are not there to service financial institutions, but are there to service other companies in trying to gain greater powers in doing that through weaknesses their bank might have exhibited.

Ms. Litan:

So, the sponsorship into the ACH system is what you are talking about?

Mr. Oliver:

Yes, I am talking about the sponsorship into the ACH system. We have to do a lot more work there. Because, despite all of this about know your customer, you are right. Education is a really hard thing. You can buy them books, send them to school, they still beat the teacher, and that is what is happening in many cases today. And it is a weakest-link issue. There are plenty of institutions out there who are not aware of the dangers.

Ms. Litan:

Is it exacerbated by the fact that now you have these Web and telephone transactions that you did not have before?

Mr. Oliver:

Yes, I think it is. With telephone transactions, there is no getting away from the fact there are a lot of people in the telemarketing business that are not doing good things. They are using the system, and most of the unauthorized return information comes out of that venue. The Web has not been as bad as it seems. The issue is that there are huge beneficial uses of the Web. Companies are doing good things in using the Web for payments transactions, online bill payment, and so forth. So, you have to be careful to segregate it here. Has it increased the risk profile? Yes. Is it possible to manage it? I think so.

Ms. Litan:

Then, one final question. The whole nature of check and ACH is a batch transaction system. Is it impossible to build real-time validations into the system? Is that a doable project?

Mr. Oliver:

That is a great question. We talk about it a lot. I will give you my opinion. Where technology will take us in the future, I do not know. But the volumes of payments we are talking about on a daily basis here in the check and ACH environment are daunting. For the central service providers to try to do that type of thing would appear today to

not be viable because it would drive the costs of those payments so high they would begin to approach the cost of the other types of transactions that are available, like wire transfers. So, there is a balance to be struck. Not today, I do not think.

Ms. Litan:

So, the back-end fraud detection scenario really does not play in so much because you do not have enough information to do it, right?

Mr. Oliver:

Well, we are improving that. We are improving the information content and everything. I think you can do a lot with back-end. What you can do on checks with back-end is a more serious issue and more difficult.

Ms. Litan:

So, it is more like you cannot put real-time validations in?

Mr. Oliver:

I would not make the statement today that it would be a thing we could do.

Ms. Litan:

Well, your job must be very challenging.

Mr. Oliver:

It is interesting.

Ms. Litan:

Now, Jim, would you like to go ahead?