Mitigating Automated Clearinghouse Fraud and Risk

November 2009

Moderator: *Welcome to Federal Reserve Bank of Atlanta's Payment Spotlight podcast. Today we're joined by Mary Gilmeister, president of the Wisconsin ACH Association, or WACHA. Mary also serves on the advisory group with the Atlanta Fed's Retail Payments Risk Forum. She will be speaking about ACH fraud and risk. Mary, thank you for joining us.*

Mary Gilmeister: Thank you, Jennifer, and I'm very happy to be a part of this podcast and to help inform financial institutions.

Moderator: *Well, Mary, although many people may have heard of the National ACH Association, or NACHA, they may not be aware that there are 18 regional payments associations across the country. What is the role of a regional payments association like WACHA?*

Gilmeister: The role of the RPAs, our abbreviation for the regional payments association, is really to provide education and support for our members on payment systems, primarily ACH, check, cards, and wire. And when our members call us, we answer their question as it relates to these different payment systems and help them resolve their issues with their customers and members.

Moderator: *Well, Mary, as you know, the ACH network has a longstanding reputation for being a safe, reliable, and secure payment system. However, in recent months there have been reports of fraudsters targeting small businesses through the ACH. What can financial institutions and their customers do to better protect themselves from this type of fraud?*

Gilmeister: Well, first of all, I would like to comment that it is a concern of ours, and a couple of my members have had some losses due to these schemes that have currently been going on with the small businesses. And we feel that some of the things that the financial institutions can do to protect themselves as well as their customers is, first of all, to provide education to their corporate customers about this scheme: How keylogging —which is the term that is currently used—works, and how important it is to have secure computers, enhanced encryption, and possibly and also including multifactor.

Another thing that a financial institution can do is to set exposure limits and to monitor those exposure limits over multidays: to make sure that when the file comes in, it is not over that file limit, and that if there was any type of unusual behaviorâ??normally, that company would not be sending in a file on a Tuesday or on a Wednesday; that would not be a payroll day or a normal day that they would be sending files. Another thing that a financial institution can do is provide callbacks. Verify that that's the file that they actually want sent, and that can also be done via fax. And also, [use] layered security to make sure that you do have multifactor security.

Moderator: *There are also less sophisticated payments fraud techniques being perpetrated against consumers, such as those targeting vulnerable groups like the elderly. In this regard, you've been working with the state of Wisconsin to develop a program that addresses the issue of financial exploitation of the elderly. What are the primary goals of this initiative?*

Gilmeister: Well, first of all, elder abuse is a very common crime. Actually, there were 5 million victims annually in the United States alone. In Wisconsin between 1995 and 2005, the total reports actually increased by 142 percent. The group that I'm currently involved with is with the state of Wisconsin, and we would like to provide educationâ??not only to consumers but also to financial institutionsâ??on early intervention, as far as what to look for, what are some of the trends with the person coming in constantly asking for cashiers checks to have things repaired. Sometimes it is a family member. So one of things that we have been providing is informational brochures to the front-line staff of a financial institution.

We also have creative training programs for the customers and members of the financial institutions if they have, for example, a gold club, where we will go in and do education and training. And they have found that to be extremely valuable so that when they're informedâ??and the financial institution is informedâ??we can work together to try to protect the elderly.

Moderator: *Now, Mary, in addition to your role as president of WACHA, you also serve on several national committees, including NACHA's Risk Management Advisory Group, or RMAG. What is RMAG's role in mitigating risk in the ACH network?*

Gilmeister: RMAG's role is representation of NACHA staff as well as financial institutions and regional payment associations, and our role is to really provide education. We have a newsletter that is produced on a monthly basis. We develop rules, and just recently NACHA passed a direct-access registration, where a third party is usually allowed direct access into the network, which increases the risk of that transaction. It is also included in the FFIEC [Federal Financial Institutions Examination Council] guidance under OCC [Office of the Comptroller of the Currency] to really monitor those types of relationships, so we develop rules. We also look at different products and services that can maybe be offered into the network. But again, it's primarily awareness, education, how to work together with the financial institutions, and what we can do to educate the businesses as well as the financial institutions of the risks that could come into the network.

Moderator: *Now, there are many changes occurring in the payment system as emerging technologies, like mobile payments and remote deposit capture, become more widely adopted. In the context of evolving payments innovation are there any payments risk issues that cause you concern?*

Gilmeister: There are a couple of them. I think the first thing is that with remote deposit capture, it is a new payment system and not a new product, and the holder of the check is now the merchant or the corporation, which adds a lot of additive risk, especially if the checks would

happen to be stolen. There are identity theft issues because now they have that person's name, address, sometimes a phone number, and sometimes merchants put a drivers license [number] on those checks, as well as the routing number and the account number.

I think one of the new and upcoming products that's being examined is consumer RDC [remote deposit capture] through the mobile, through the telephone. I have calls that are dropped all the time, so I'm not sure how that's going to play into the picture. But I think that the consumersâ?¦what are they going to do with those particular checks? How are they going to destroy those checks? Are they just going to end up accidentally throwing them in their trash, and they're picked up by other people? I think that's a concern we have: the identity theft and the increased awareness that these items could be not in the financial institutions' hands anymore; they're actually in the consumer's hand.

I think another area of risk is the use of third-party processors and companies. Granted, at WACHA, as a company, we use a third party. When you start using third partiesâ??and the more third parties you have, the less closeness you have to working directly with your financial institution and their productsâ??I think that also brings additional risk, especially in today's economic environment. And a lot of times the third parties don't necessarily have the regulatory guidance that many of our financial institutions have, so I think that as the payment systems move further away from the financial institution there is going to be increased risk.

Moderator: *Thanks, Mary.*

Gilmeister: Thank you.

Moderator: *Again, we've been speaking today with Mary Gilmeister, president of the Wisconsin ACH Association. This concludes our Payments Spotlight podcast on ACH fraud and risk. On our Web site, frbatlanta.org/rprf, you can read more about the Retail Payments Risk Forum. Thanks for listening, and please return for more podcasts. If you have comments, please send us an e-mail at podcast@frbatlanta.org.*