VOLUME FIVE, NUMBER TWO • DIGITAL TRANSACTIONS.NET • FEBRUARY 2008

DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

The Broken Link

How a radically new species of debit card severs the crucial tie between banks and demand deposit accounts.

ALSO IN THIS ISSUE:

- The Specter of Interchange Regs
- Selling Back Office Conversion
- ATMs That Dispense Gift Cards
- Arming Consumers to Fight Fraud

The Big Risk in Instant Account Verification

George F. Thomas

Non-account-holding banks are starting to ask consumers for their passwords and other log-on credentials to make sure they own the accounts they're using to make payments. At a time of massive data breaches, this is a dangerous practice that should stop now.

As long as online access has existed, consumers and employees have been instructed to protect their user codes and passwords. The usual advice is: Don't write the user code and password down, make sure that the password is complex enough so that it cannot be guessed, don't use birth dates, family-member names, pet names, and so on.

Financial institutions are now taking the next step by adding additional levels of log-on protection known as multifactor authentication.

So why are financial institutions asking their customers for the online-banking credentials they use at another financial institution? It may sound crazy, but it's going on today. One of my financial institutions recently asked for my log-on credentials to validate my accounts at one of my other financial institutions when I enrolled for an external funds transfer service. Thankfully, the bank also provided another secure method of account verification, though it took a couple of days.

The big question is: How many consumers understand the danger of giving this information out, especially when they are not given an alternative method of authentication?

Without a doubt, validating that a bank account belongs to a given individual is a difficult task. There are no databases in existence that can give real-time assurance that the bank account that individuals are providing for online bill payment, funds transfers, or online purchases actually belongs to them. They could easily provide a corporate bank account or an account of another individual.

How many consumers understand the danger of giving this information out?

But the lack of a real-time capability should not make it an acceptable industry practice to ask consumers for their banking credentials.

A Resounding 'No'

A recent press release by Obopay Inc. and Yodlee Inc. on what they call "Instant Bank Account Verification" illustrates that this practice for account validation is becoming more widely accepted. Here's an excerpt: *"Yodlee's Account Verification lets Obopay users authenticate bank account ownership in real time by entering their online banking user name and password. Yodlee currently provides ownership confirmation for bank accounts at more than 650 financial institutions that carry more than 80% of American account volume. This information is confirmed by Obopay through Yodlee in a matter of seconds. Once confirmed, Obopay users can immediately begin sending money between their Obopay account and their existing bank account."*

And it's not just Yodlee. Other companies are offering a similar service.

Now, some regular users of such services may not fret all that much about it. "For the rightfully paranoid, Yodlee is probably a target for hackers trying to get at all those passwords," said one consumer, writing on a money blog recently. "But since I log in just about every day to keep track of my many accounts, any sort of unauthorized withdrawal will be noticed immediately. And I figure it's just as likely that someone will

hack into my bank's Web site as Yodlee's, so at least this way I can nip it in the bud." But the point that this consumer is missing is that the passwords for all of his accounts are now with Yodlee. It is easier to hack into one database than many.

As all the recent news about data breaches has shown us, consumer data is hard to keep safe. And a data breach involving consumers' online-banking credentials would damage the payments industry immensely.

It's not difficult to see how such data can pile up quickly. After all, when a trusted entity like a financial institution asks its customers for their log-on credentials at another institution, most customers probably would not think twice about it because the request is coming from a trusted party.

But a requesting financial institution should be able to answer some questions, such as:

- Who has access to the log-in credentials at the financial institution or service provider?
- How many people can see it?
- How is it protected?
- How long is it maintained?
- Who has the liability?
- Who has the reputation risk?
- Do you want your customers giving their log-on information to other institutions?

The answer to the last answer should be a resounding "no." Senior management in most of these financial institutions would probably shudder if they were informed that their institution was requesting the log-on credentials at other financial institutions as part of their services.

Banks at Risk

The consumer is giving up a lot when he signs up for this sort of account-verification service. The following excerpt comes from the additional terms agreed to by the consumer for the account-verification service with Yodlee and Obopay:

"By using the Account Verification Service, you authorize Obopay and its supplier Yodlee, Inc. ("Yodlee") to access third party sites designated by you, on your behalf, to retrieve information requested by you. For all purposes hereof, you hereby grant Obopay and Yodlee a limited power of attorney, and you hereby appoint Obopay and Yodlee as your true and lawful attorney-in-fact and agent, with full power of substitution and re-substitution, for you and in your name, place and stead, in any and all capacities, to access third party internet sites, servers or documents, retrieve information, and use your information, all as described above, with the full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection with such activities, as fully to all intents and purposes as you might or could do in person."

Even if a similar type of agreement were in place with the financial institution, the liability for security breaches and fraud as a result of misuse of the log-on credentials should fall squarely on the shoulders of the requesting financial institution.

But the reality is that the account holder's financial institution—which is an innocent party in all of this, especially if it is not aware that its customer gave out confidential information at the request of another financial institution—is also at risk.

Account-holding financial institutions must continue to educate their customers. They should inform them that they should never divulge their online credentials to third parties, not even to another financial institution. Another step they should take is to advance their multifactor authentication programs to prevent this practice from continuing.

Above all, requesting financial institutions should stop this practice altogether and instead rely on methods like challenge-account verification, which may take a little longer but has none of the risks of requesting log-on credentials. Challenge-account verification usually occurs when random low-value transfers are sent to the consumer's account, after which the consumer must verify the amounts.

Instant account verification is not essential and is surely not worth the inherent risks. DT

A data breach involving consumers' online-banking credentials would damage the payments industry immensely.

Instant account verification is not essential and is surely not worth the inherent risks.

George F. Thomas is chief executive of Radix Consulting, Oakdale, N.Y. Reach him at gfthomas@radixconsulting.com.