

Comments on FDIC Report
“Putting an End to Account-Hijacking Identity Theft”

Bob Pinheiro

Robert Pinheiro Consulting LLC

As the FDIC report points out, “account hijacking” occurs when an individual’s personal information is misused by criminals, allowing them to impersonate a bank account’s rightful owner and thereby gain access to the account. Because many banks now provide online bill paying services to their retail customers, it’s a simple matter for thieves to create fraudulent payment transactions and drain the victim’s account, once the thief is in possession of the victim’s account information. In the case of account hijacking, the misused information likely consists of account login IDs and passwords. However, the ability to misuse personal information to conduct financial fraud extends far beyond account hijackings. Identity theft is perhaps the most well-known example. A criminal who obtains personal information about someone, such as a social security number, is able to create new credit accounts in the victim’s name. **This is largely because “proof of identity” too often means nothing more than knowledge of a social security number.**

Most people are familiar with the fact that a thief who obtains their credit card information can easily run up bogus charges on the victim’s credit card, especially if the stolen information includes the “security code” printed on the card. But many people may not be aware that thieves can steal money from their checking accounts using nothing more than knowledge of their checking account numbers. One way this happens is when paper checks are converted into “electronic checks”, usually by merchants receiving the checks who want to receive faster payment. With electronic check conversion, the check writer’s bank is no longer presented with a paper check with an authorizing signature on it (or even an image of the check). The bank only receives an electronic request for payment from the merchant’s bank, via the banking industry’s ACH (Automated Clearing House) network. This state of affairs provides opportunities for criminals who steal checking account numbers and use the information to create bogus checks, which can then be converted into ACH transactions. Criminals armed with checking account information can also make purchases online, or over the telephone, from merchants who can initiate ACH transactions and are willing to accept checking account numbers for payment purposes. The misuse of checking account information has such potential to enable criminals to drain people’s accounts that NACHA, the national organization that sets the rules for electronic funds transfers, has issued a warning on its website, alerting people to safeguard their checking account information. Yet this information is printed on every paper check that people use to pay their everyday bills.

All these examples – account hijacking, identity theft, credit card fraud, and ACH fraud – share a common theme, which is that the security of our identities and financial accounts depends on keeping our personal information out of the wrong hands. In other words,

our security is dependent on keeping sensitive personal information secret. But identity thieves have multiple ways to get the information they need. There's "dumpster diving", whereby thieves rummage through the trash looking for personal information they can use. People lose wallets. Corporate employees can steal information about people that is contained in company databases. Commercial and government databases contain a wealth of personal information that criminals can tap into. Keystroke logging programs can inadvertently be installed on personal computers, allowing everything typed in (including login IDs and passwords) to be seen by criminals. And now thieves can resort to "phishing", those official-looking e-mails that try to trick people into divulging account numbers, passwords, social security numbers, and other personal information.

The financial services industry has adopted several approaches to dealing with these problems. One approach is to implement fraud detection systems that monitor account activity for patterns that are inconsistent with patterns of previous transactions, thereby indicating potentially fraudulent transactions. Another approach is to warn consumers to better safeguard their personal information and to dispose of documents containing sensitive information by shredding them. A third approach has been to ask customers to monitor their financial account activity more closely, so that fraud can be caught early. Another approach is to offer services to fraud victims to help them undo the damage. For instance, the Identity Theft Assistance Corporation was started by the industry to provide this assistance to victims. **Yet none of these approaches really address the basic problem, which is that knowledge of a few pieces of personal information that can be obtained by thieves with little difficulty is often accepted as "proof" of one's identity, and enables account hijacking and other financial fraud.**

A recent report sponsored by several financial institutions appears to support the approach that the financial services industry seems to be taking in dealing with identity fraud in general. The report, "2005 Identity Fraud Survey Report", by Javelin Strategy & Research, states that, "although there has been much recent public concern over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels.....Conventional methods such as through lost or stolen wallets, misappropriation by family and friends, and theft of paper mail are among the most common ways thieves gain access to information." The gist of Javelin's recommendations for dealing with identity fraud is for consumers to: (a) better safeguard sensitive personal information from loss or theft, (b) conduct more financial transactions online rather through paper channels, and (c) better monitor their account activities so that fraud can be detected early. Javelin's recommendations to financial institutions is largely limited to providing more education to consumers about how to protect personal information and detect fraud early, and to make it easier for consumers to detect fraud early by streamlining online reports and other documentation. The Javelin report (at least the shortened, complementary version available on Javelin's website) does not address authentication as an option for dealing with identity fraud, although it does recommend that financial institutions initiate email and phone notifications to alert consumers when suspicious account activity is detected.

Even with Javelin's assertion that most personal information used to enable identity fraud is obtained offline, it seems reasonable to expect that as consumers increasingly conduct online financial transactions (as Javelin recommends), the opportunities for online theft of personal information will increase. As stated in the FDIC study, "Thus, although the problem of account hijacking is as yet relatively small, it is nonetheless serious for customers (both retail and commercial) and for financial institutions. The increasing access to alternative electronic payment systems means an increasing number of access points to financial institution systems, with each access point representing a pathway for a potential security breach. The increasing number of access points, coupled with the potential for anonymity afforded by electronic payment systems, facilitates electronic banking fraud."

What's really needed to prevent account hijacking and other fraud enabled by stolen personal information is a way to make this information less useful to criminals for committing fraud. The FDIC report addresses this view head-on by recommending that two-factor authentication ought to replace single-factor authentication as the means by which people verify their identities for access to online financial accounts. It's well known and generally acknowledged that single-factor authentication, whereby a person "proves" their identity by demonstrating knowledge of a password, provides weaker security than two-factor authentication. With two-factor authentication, the consumer, who presumably has already verified his identity to the bank's satisfaction when setting up an account, is issued an authentication "token." Now, in order to access an online account, a customer not only must know a password or PIN (personal identification number), but must also demonstrate possession and control of the token¹. When two-factor authentication is used, mere knowledge of personal and account information becomes much less useful as fraud enablers. Many banks do, in fact, use two-factor authentication for their commercial and business customers who conduct high-value transactions online. If two-factor authentication offers more security than single-factor authentication, and is already being used to secure high-value business accounts, then why can't it also be used to protect consumer accounts from being hijacked and drained of funds?

Before considering that question, it must be noted that two-factor authentication alone does not necessarily solve the problem, because of the possibility of "man-in-the-middle" attacks. For instance, the banking customer may believe he is trying to access his account from the bank's website, but is really communicating with a fraudster's site. So even if one-time passwords generated by an authentication token are used for two-factor authentication, the fraudster can gather this information and immediately provide it to the legitimate bank website, thereby accessing the customer's account. **To guard against man-in-the-middle attacks, it is imperative that the bank's website also be authenticated to the customer**, so that the customer does not provide login information to a fraudulent website. For instance, the bank's website might display a picture that was provided by the customer to the bank, and that wouldn't be known to a fraudster. Commercial vendors offer various solutions that allow a website to authenticate itself to a

¹ For instance, the token may display a different "one-time password" every minute. Providing the one-time password at a given point in time demonstrates possession of the token.

user. Naturally, this requires some additional customer education, so that customers will recognize when they are dealing with a legitimate banking website.

The stumbling blocks to using two-factor authentication at the consumer level include cost, complexity, and consumer acceptance. In response to the FDIC report, the financial services industry may point out that deployment of two-factor authentication for online consumer banking would be an expensive and complex undertaking, since a great many accounts would be affected. The industry may respond that the financial losses suffered due to account hijackings do not merit the expense it would take to deploy two-factor authentication. The industry might also respond that the problem of account hijacking is less severe than other types of fraud that is enabled by stolen information, such as credit card fraud, and that their customers may not want to be bothered with more stringent authentication requirements before accessing their accounts online. These are legitimate points and must be addressed before it becomes practical for banks to implement stronger forms of authentication for their consumer banking customers.

A 2003 NACHA report entitled “Internet Payments Fraud: A Primer for Merchants and Financial Institutions”, also suggests that consumers need to keep their personal information safe and should monitor their financial accounts to detect fraud early. However, the NACHA report also suggests that financial institutions employ authentication to prevent fraud: “Since fraudsters may attempt to obtain information directly from FIs, customer authentication is critical at the time of account opening and during all subsequent interactions. Financial institutions should authenticate customers by requiring proof of account ownership, rather than simply knowledge of an account number. Financial institutions can use usernames, PIN numbers, and passwords to authenticate existing customers, which provides a higher level of security than is possible with publicly-available information, such as social security numbers.” Although the NACHA report does not address two-factor authentication, the tone of the report would seem to be sympathetic to FDIC’s recommendations.

What Financial Institutions Should Do

It is certainly better, at least from a victimized banking customer’s point of view, to prevent account hijacking in the first place, rather than deal with the damage after the money has been siphoned away. Even if financial institutions are protected against losses by insurance when accounts are broken into and money stolen, financial institutions still need to be sensitive to the inconvenience and hardships that account hijacking will cause to their retail customers. Insurers might also decide, at some point, that their coverage for losses due to fraud should be dependent on measures taken by financial institutions to prevent fraud.

One way to prevent account hijacking is obviously to eliminate the fraudsters and shut down their operations. While this is a laudable goal, it will never be fully realized. Other than eliminating the fraudsters, prevention would then seem to depend on two basic strategies: either find better ways to keep sensitive personal information secret so that fraudsters can’t get it and commit fraud, or else find ways to make such information less

useful in enabling fraud. It was noted previously that thieves have numerous ways to obtain personal information about people. Although customers should certainly be encouraged to keep their information secure, reliance on better protection of information alone should not be the dominant strategy. Instead, **financial institutions should focus on a strategy of ensuring that mere knowledge of sensitive information alone is not sufficient to commit identity fraud, including account hijackings.** This can be done by adopting “better mutual authentication”², a term defined by the Financial Services Technology Consortium that includes two-factor authentication, as recommended by the FDIC, in combination with authentication of bank websites to online customers.

An industry-wide effort should be undertaken to rigorously investigate the options for deploying better mutual authentication for consumer banking applications, including feasibility issues and costs of various deployment alternatives for two-factor authentication. For instance, there are a variety of ways to implement an authentication token, some more expensive than others. These include one-time password tokens that can be affixed to one’s key chain, USB tokens embodying cryptographic keys, “soft tokens” residing on a computer’s hard drive, high-end cell phone, or personal digital assistant, and even paper cards containing printed one-time passcodes. The Financial Services Technology Consortium is currently planning to undertake a “Better Mutual Authentication” initiative. This could serve as a valuable first-step in an industry-wide effort to understand how stronger forms of authentication could be deployed and used by consumer banking customers.

In considering options specifically for deployment of two-factor authentication, the financial services industry should investigate whether potential cost savings or other benefits may accrue if some banks are able to provide authentication services to other banks, thereby relieving those banks from having to implement and manage all aspects of two-factor authentication. For example, a large bank may act as a “credential service provider” by providing one-time password tokens to customers of smaller banks. Once the smaller bank registers a token as belonging to one of its customers, those tokens may be used to authenticate the holder when accessing accounts at the smaller bank. In effect, the smaller bank would rely on an authentication service provided by the larger bank. A new non-profit organization, the Electronic Authentication Partnership, is defining rules and criteria by which non-affiliated relying parties and credential providers may enter into trust relationships. Such trust relationships could form the basis for “interoperable credentials” that consumers would possess, and that could be used to authenticate the holder’s identity at any financial institution where the individual has an account.

The concept of interoperable credentials may also be appealing from a customer’s point of view. If better mutual authentication is “good” and becomes increasingly deployed by financial institutions, a situation will arise whereby individual consumers will become burdened by multiple authentication tokens, each useful at only one institution. It would be more efficient, and less cumbersome, if a single token could be used for authentication at multiple institutions.

² “Understanding and Countering the Phishing Threat”, Project Whitepaper of the Financial Services Technology Consortium, 1/31/2005

The idea that some banks would act as credential providers to other, unrelated entities has a precedent in the government's E-Authentication initiative. E-Authentication would allow government agencies to authenticate the identities of individuals seeking to use certain government services online by allowing those agencies to rely on bank-issued credentials.

A longer-term benefit of interoperable credentials could help to prevent identity theft. One reason why identity theft is such a relatively easy crime is that creditors have no easy way to authenticate the identities of people they don't know who are seeking to open new accounts. But people who have bank accounts already have an established and trusted relationship with those banks. Interoperable banking credentials supporting two-factor authentication could help prevent identity theft if banks would be willing to act as "trusted authenticators" on behalf of their customers. Creditors could check to determine whether the identity being claimed by an applicant for a new account is associated with interoperable credentials issued by some bank or other financial institution. The creditor could then request the bank to authenticate the account applicant's credentials to determine whether the applicant and the person whose identity is claimed possess the same credentials and are, therefore, the same person.

Bob Pinheiro

Robert Pinheiro Consulting LLC
bp@bobpinheiro.com