Preventing Identity Theft Using Trusted Authenticators

Robert Pinheiro , GSEC
Independent Security Researcher
bp@bobpinheiro.com

Abstract

Identity theft is a crime that is enabled by two faulty assumptions about the way that the identity of a person is verified in our society. The first is that someone who demonstrates a knowledge of certain items of information about a particular person is presumed to be that person. The second assumption, which gives rise to the first assumption, is that these items of information can be kept confidential. Because identity thieves often seek to open new credit accounts using their victim's personal information, this paper proposes a method for authenticating an application for a new credit account that does not depend on these assumptions. The proposed method determines whether the new account applicant is truly the person named in the application, via a "trusted authenticator" designated by the latter individual. It is suggested that a viable candidate for a person's trusted authenticator can be found within the financial services community; in particular, a bank or other financial institution with whom the individual has a trusted relationship, such as a bank account.

The Problem

Identity theft is a growing national concern, both in terms of its affect on its victims, and its potential national security implications. A report issued in September 2003 by the Federal Trade Commission estimates that almost 10 million Americans were victims of some type of identity theft within the previous year[1]. Especially unnerving are the numerous accounts of the ordeals that victims endure as they attempt to deal with the results of this crime[2]. They are assumed to be responsible for the debts incurred by the thief until they can demonstrate that they have been victims of fraud. They are targeted by collection agencies trying to collect on debts generated by thieves who open new accounts in their name. They have to deal with damaging information placed in their credit files as a result of the imposter's actions. They may even find themselves the subject of an arrest warrant, if the identity thief used their name and personal information for identification to the police at the time of an arrest.

It's well known how this can happen. Fraudulent charges may be posted to someone's credit card account if the thief knows the account number and expiration date. Identity thieves can "take over" an existing account and withdraw money, as well as change other account information such as mailing address, if the thief knows a few pieces of sensitive personal information, especially the account holder's Social Security Number (SSN).

[1] Federal Trade Commission Identity Theft Survey Report, September 2003, page 4
[2] See www.privacyrights.org/cases/victim.htm

Perhaps worst of all, a thief can easily open a new account in someone else's name by completing an application for a new credit account, using the victim's name and SSN, but with a different address. The credit grantor, whether it be a retailer offering instant credit accounts via their website, a telecommunications company offering a new cell phone account, a bank offering a credit card, or an auto dealership offering a new car loan, uses the information provided by the thief to obtain a credit report on the person named in the account application. If the report indicates that the person named in the application is a good credit risk, a new account will likely be opened in the victim's name. But the victim never knows about the late and unpaid bills, until his credit is ruined.

Identity theft happens because creditors assume that the person applying for a new account is the same person whose name and personal information are used in the application, unless there is clear evidence to the contrary. A creditor "authenticates" an applicant for credit by matching personal information provided in the application, such as name, SSN, birthdate, etc., with information contained in a credit report. If there is a match on at least a few items of information, it is assumed that the person making the application is the same person whose credit history is contained in the credit report. This assumption itself is a direct result of a belief that sensitive personal information can be kept secret and out of the hands of thieves. Yet the widespread incidence of identity theft, as detailed by the personal stories of its many victims, clearly demonstrates that this notion is false. A recent paper by Prof. Daniel Solove of the Seton Hall Law School aptly points out that "The identity thief's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in the collection, dissemination, and use of that information[3]." He further goes on to say "The problem, however, runs deeper than the public disclosure of SSNs and personal information. The problem stems not only from the government's creation of a de facto identifier and lax protection of it, but also from the private sector's inadequate security measures in handling personal information……Further, identity thieves can obtain SSNs and other personal information simply by paying a small fee to various database companies and obtaining a detailed dossier about their victims[4]."

There's only a certain amount that an individual can do to prevent sensitive information from getting into the wrong hands, such as keeping a tight grip on one's purse or wallet. Beyond that, the information is easily available to a thief in numerous other ways. It may be available through certain public records. It can be purchased from publicly available databases for a nominal fee. It can be copied from medical claims forms lying around in a doctor's office. Victims and others can be tricked into providing sensitive information to a thief who uses "social engineering." For instance, a thief can call a victim's bank or other creditor, and convince the representative that the thief is, in fact, the person whose account the thief is trying to steal. Calls may also be placed to individuals themselves, in an attempt to trick the individual into providing personal information by pretending to

[3] Solove, Daniel A., "Identity Theft, Privacy, and the Architecture of Vulnerability", Hastings Law Journal, Vol 54, N o. 4 (2003), page 1251
[4] see Solove, supra note 3, page 1255

need the information for a valid-sounding purpose. Other methods include breaking into various commercial databases containing sensitive information about a business's customers, many times with the help of someone on the "inside."

As long as the authentication of new credit applications is based upon knowledge of a few items of personal information that are supposed to be confidential, the only way to truly prevent this type of identity theft is to keep one's personal information out of the hands of thieves, an impossible task. This is also true in the case of identity theft involving account takeovers, in which the thief uses knowledge of personal information about the victim to obtain information needed to take over someone's existing account.

Possible Solutions

A frequently suggested solution to the identity theft problem is to enact laws restricting the availability and usage of sensitive personal information such as SSNs. Such efforts may help to prevent some identity theft in the short run. However, attempting to limit the distribution and availability of personal information cannot be a long-term solution to the identity theft problem as long as the integrity of the credit-granting process depends on the false notion that one's personal information can be kept secret. Much of this sensitive information is already "out there" in one place or another, making it very difficult to ensure that the information can be kept confidential and away from identity thieves. As previously noted, thieves can always find a way to obtain sensitive information through devious, if not illegal, means. And while limiting the distribution and availability of sensitive information may be desirable from the standpoint of personal privacy, others argue that such information is needed for legitimate purposes such as locating missing persons, fraud investigations, identifying landowners and other property owners, background and pre-employment screening, and a host of other reasons.

Other efforts to thwart identity theft include proposals for allowing states to adopt stronger financial privacy laws than federal law allows, laws providing for free credit reports once a year, and laws making it easier for consumers to ensure the accuracy of the information contained in their credit reports. These are all worthwhile efforts, and certainly go a long way toward helping consumers monitor their credit status, as well as clean up the mess resulting from an identity theft. However, as long as creditors continue to assume that a person's identity is authenticated by knowledge of a SSN or other personal information, such laws really don't address the core problem that enables identity theft. The identity theft solution must depend on stronger forms of authentication to verify the identity of those applying for new accounts, or those attempting to modify existing accounts.

It would seem that a big chunk of the identity theft problem could be eliminated if credit grantors took greater pains to better authenticate applicants for new accounts. Couldn't creditors check to determine if the person whose name and SSN are given in a new account application is truly the person who submitted the application? There are at least two reasons why creditors typically don't do this, or do so only when other suspicions have been raised. The first is that, using today's methods, it's difficult and time

consuming to authenticate someone applying for a new account online, or over the phone, or even through the postal mail. The creditor doesn't know the person, and has limited means to make such an authentication. As noted previously, one such method is to match pieces of information provided in the application against information contained in a credit report. However, creditors do not always match all available pieces of information, especially addresses. Although this method of authentication could be strengthened if more "points of identity" were matched, there are no uniform laws or regulations governing this. A second reason is that the liability of creditors is limited. If a mistake is made by the creditor and an account is opened for an imposter, the creditor is not liable for damages to the person whose identity was stolen. All too often, the costs of dealing with these fraudulent accounts have simply been regarded by creditors as part of the cost of doing business, and passed along to other customers in the form of higher prices, fees, and interest rates.

Several approaches to curbing identity theft are voluntarily being taken by the financial services industry. Some of these involve detecting discrepancies in the information provided in a credit application, checking the information provided against known fraud information, and reviewing the credit report for a possible Consumer Alert or Fraud Alert reported by a consumer. Others involve various types of fraud scores that can be computed and assigned to an application, based on analytical models of fraudulent behaviors. Although useful, these procedures may not be employed unless the application is considered to be suspicious. Moreover, creditors that are not financial institutions, such as retail stores, may not employ them at all. Perhaps most importantly, because these methods depend on detecting some problem or pattern of misuse involving the information provided in the application, they would not prevent fraud from occurring with applications that do not trigger these defenses. For instance, fraud scores would seem to have a low likelihood of detecting a fraudulent account application in the name of someone who had not previously been an identity theft victim. Presumably, there would be no existing problem or pattern of misuse associated with such an application.

Another approach involves fraud-detection services that gather various types of "out-of-wallet" information about someone named in a credit application. Credit bureaus, in fact, offer such services to their customers (i.e., those who use credit reports for making decisions about creditworthiness). For instance, an identity thief is unlikely to know the name of the victim's home mortgage lender, or the amount of a recent check written by the victim. So a credit applicant may be asked to name his or her mortgage lender, or the amount of the recent check, if sufficient suspicions are aroused about the application. This is similar to the "knowledge-based authentication" approach suggested by Willox and Regan[5]. As they state in their paper, "a successful knowledge-based authentication solution is dependent upon the ability of the verifier to possess a sufficient quantity of information pertaining to individuals, from which the verifier can determine whether a subject person is who he or she says they are." However, creditors must first subscribe to a service that provides such information, which they may not do. When creditors do subscribe, contacting new account applicants and asking out-of-wallet questions is most

[5] Willox, Norman A. and Regan, Thomas M., "Identity Fraud: Providing a Solution", Journal of Economic Crime Management, Volume 1, Issue 1, Summer 2002.

likely to be used only to verify suspicious applications. And even if out-of-wallet questions were to be asked of each and every new account applicant, this approach still relies on the underlying premise that sensitive personal information can be kept out of the hands of identity thieves. Surely sophisticated thieves can find ways to gather this information themselves. In addition, the widespread sharing of personal information that would be necessary to enable this knowledge-based approach to authentication may raise privacy concerns among consumers, privacy advocates, and lawmakers.

While these approaches may help in reducing the number of fraudulent account openings, the statistics regarding the alarming growth of identity theft speak for themselves: such methods are either not used widely enough to prevent the identity theft that does occur, or are simply inadequate to have much of an impact.

A recent paper by Prof. Lynn LoPucki of the UCLA School of Law[6] addresses many of the concerns raised in this paper, and suggests an approach to the identity theft problem that addresses the fundamental flaws in the process. This approach does not depend on keeping personal information secret, asking out-of-wallet questions, or computing fraud scores based on historical data and analytical fraud models. LoPucki's approach, which he calls the Public Identity System (PIDS)[7] would establish a voluntary list of people concerned about identity theft, and who consent to be directly contacted for verification when someone applies for credit in their name. The list would be maintained by a government agency. An individual would voluntarily provide his/her personal information to the list, including name, SSN, and perhaps other identifying information. A thorough authentication process would ensure that new members of the list are truly the persons they claim to be. A personal appearance before the government agency that maintains the list would be required. Individuals participating in PIDS would specify one or more standardized ways that a creditor should contact them when the creditor has received a new account application in their name. Contact methods would likely be limited to a phone call, e-mail (encrypted or unencrypted), or US Mail.

When a creditor receives a new account application, the creditor would consult the list to determine if the person named in the application, as identified by a SSN or other information, is a PIDS participant. If the named person is not a participant, the new account application would be processed in the usual manner. If, however, the named person is a PIDS participant, the creditor would contact the individual directly using one or more of the contact methods specified in the instructions provided by the individual. A PIDS participant may even require, under some circumstances, a personal appearance before the creditor by anyone applying for a new account in his or her name. The reason for contacting the participant would be to verify that the participant is truly the person who submitted the new account application.

To significantly reduce identity theft using this approach, creditors would need to have an incentive to consult the list and follow the instructions given, and consumers would need

[6] LoPucki, Lynn M., "Human Identification Theory and the Identity Theft Problem," 80 Tex. L. Rev. 89, (Nov. 2001), available at ssrn.com/abstract=263213
[7] LoPucki, Lynn M, "Did Privacy Cause Identity Theft?", Hastings Law Journal, Vol 54, No 4, April 2003

to participate in PIDS in large numbers. Although consumers have signed up in massive numbers with the recently established Do Not Call list maintained by the Federal Trade Commission, this is most likely because people have dealt with telemarketers and want to avoid future interactions. But the people who should be first in line to join PIDS; i.e., those whose identities have not yet been stolen, will not have had the very negative experience that would perhaps motivate others who have already been victims.

Although PIDS participation would be voluntary on the part of consumers, strong incentives should exist for creditors, when processing account applications, to query the list and follow any authentication instructions given. Prof. LoPucki suggests that such an incentive would consist of amending laws such as the Fair Credit Reporting Act (FCRA) to make creditors liable for damages if a PIDS participant is named in a new account application, and subsequently becomes an identity theft victim because the creditor failed to use the PIDS list to verify that the participant actually filed the application.

Although Prof. LoPucki's approach addresses the fundamental flaws in the credit-granting process responsible for identity theft, some difficulties may arise with its implementation. The list of PIDS participants, together with their SSNs and contact information, would reside on a government website, and the information would be available to the public. This would only be implemented if the laws were changed to prevent knowledge of this information alone as providing "proof" of identity, as well as preventing other types of privacy invasions that might be enabled with public access to such information. Although the legal changes would make one's personal information much less useful to an identity thief, it is not clear how comfortable people would feel about an arrangement that allows their personal information to be made public in such an overt manner. In addition, PIDS participants would also need to personally appear before the government agency managing the list. These two factors may inhibit many people from participating in PIDS.

Since creditors would be required to directly contact individuals named in an account application if the person's name appears on the list, creditors may find this type of "direct authentication" process to be burdensome, especially if it involves more than a simple phone call or email. This may lead creditors to oppose PIDS. In addition, there is the question of how the creditor should authenticate the person taking the call, or responding to the email. How can the creditor be sure that the person taking the call, or responding to the email, is truly the person who joined PIDS, and who now should be queried about the credit application?

Finally, the implementation of PIDS would seem to require the establishment of a new government bureaucracy to perform necessary functions such as establishing and maintaining the PIDS list, meeting with those individuals seeking to participate, verifying their identity credentials, and establishing the standardized methods by which creditors will contact and interact with PIDS participants. Of course, implementing any alternative to PIDS would also require a certain amount of up-front work to develop the necessary capabilities and infrastructures. And while it is not unreasonable for a government

agency (such as a state motor vehicles bureau) to undertake at least some of these tasks, it is not clear whether any federal or state agencies would be ready and willing to fulfill the entire role.

Preventing Identity Theft Using Trusted Authenticators

One possible solution to these problems may be to modify the PIDS procedure somewhat to take advantage of existing trust relationships that individuals have already established with various organizations that they deal with. Rather than requiring creditors to authenticate applicants for new accounts by contacting them directly, these interactions could instead be performed by a "trusted authenticator." The trusted authenticator would be an entity that already knows the individual, maintains personal information about that individual, and has established a trusted relationship with that person. The advantage of using trusted authenticators is that the authentication process can be built on trust relationships and infrastructures already in place. A reasonable candidate for such a trusted authenticator would be a bank or other financial institution with whom the individual has already established an account. After all, if most people trust a bank to handle their money and keep it safe, trusting that same bank to authenticate their identities in other financial transactions should be natural. Prof. LoPucki's paper hints at such an arrangement in its discussion of how list members may choose to be contacted: "The [e-mail] contact could be directly with the owner or through the owner's trusted intermediary."[8] Instead of creating a new government bureaucracy to implement PIDS, the existing infrastructures and trust relationships within the financial services community could be enhanced to more efficiently derive the same benefits that PIDS provides.

In this modified direct authentication procedure, a list of all individuals who choose to participate (the "participants") would still be needed. The list would contain a name and SSN of each participant, together with the identity of their trusted authenticator. The list would be maintained by a new organization created by the financial services community expressly for this purpose, rather than by the government. However, the information on the list would not be accessible by the general public, but only by creditors and other members of the financial services community acting as trusted authenticators. Authentication of a new account application would be achieved via a trusted authenticator acting on behalf of a participant named in the application. Although ultimately it is, or should be, creditors themselves who are responsible for authenticating those who apply for new accounts, in many cases these creditors will be banks or other members of the financial services community. So it is not unreasonable that the financial services community should have a leading role in implementing stronger forms of personal authentication for identity theft prevention.

The modified authentication procedure would tentatively work as follows:

1. The creditor, upon receiving a new account application, checks the list to determine if the person named in the application is a participant. If so, the

[8] see LoPucki, supra note 6, page 34

creditor queries the trusted authenticator designated on the list, and requests verification that the person named in the application is actually the person filing the new account application If the person is not a participant, the creditor will process the application in the usual way.

2. Upon receiving a request from a creditor for direct authentication of a participant, who is also one of its customers, the trusted authenticator contacts its customer via a secure email message or phone call, as specified by the customer.

3. When communications is established, the trusted authenticator must first determine that it is actually communicating with its customer, and not someone else who has intercepted the email or phone call.
    - An email would contain a link that takes the customer to an authentication screen on the trusted authenticator's website. Here the customer would provide a password or Personal Identification Number (PIN) to authenticate himself/herself. The authentication process may also include an additional biometric factor such as a fingerprint or voiceprint[9]. Most likely, the method of authentication used would be the same as the customer would use for online banking, which provides access to his/her banking accounts online.
    - A phone call would contain, at minimum, a request for the customer to provide a PIN or some other secret. A more secure authentication process might include an additional biometric factor, such as a voiceprint. Again, the method of authentication may be the same as the customer may use to perform telephone banking, which provides access to his/her banking accounts over the phone.

4. Once the trusted authenticator has verified the identity of its customer, it asks its customer whether he/she has filed a specific application for credit, as indicated in the creditor's request for authentication.

5. If the customer responds affirmatively, the trusted authenticator replies to the creditor that the application appears to be authentic. If the customer responds negatively, the bank responds to the creditor that the application appears to be fraudulent. Or, the trusted authenticator may simply reply to the creditor with the customer's (i.e., participant's) response.

Creditors would have the same incentive for checking the list and contacting the trusted authenticator as they would have with PIDS: exemption from liability if a new credit account is opened for an imposter. Since creditors can harm an identity theft victim's

[9] Authentication of a person is usually based on one or more of the following factors: something you know, something you have, and something you are. "Something you know" is a secret piece of information, such as a password or PIN. "Something you have" is a physical item in the person's possession. In this case, the item could refer to an email directed to the person's designated email address, or a phone call received at the person's designated phone number. "Something you are" refers to a biometric such as a fingerprint or voiceprint.

credit record by reporting erroneous and damaging information to the victim's credit bureau, it is not unreasonable that creditors should bear some responsibility for verifying the identity of those applying for new accounts.

Unlike the current method that creditors use to authenticate new credit applicants; i.e., checking various identity points in an application against a credit report, the method proposed here is a stronger form of authentication because it requires more than a knowledge of sensitive information about someone. The "secret" information required is a password or PIN, which was created by the bank's customer and will not exist in commercial databases maintaining out-of-wallet information. In addition, the customer will have received a phone call or secure e-mail from its trusted authenticator, which acts as a second factor. When biometrics are employed, this strong authentication procedure includes three factors: a secret known to the customer, such as a password; a "thing" possessed by the customer – an email or phone call from the bank; and a biometric such as a voiceprint.

Finally, although this procedure is geared to preventing identity theft as it relates to the fraudulent opening of new credit accounts, it relies on the trusted authenticator's ability to authenticate its own customer. If the trusted authenticator is a bank or other financial institution, it is also concerned about identity theft that involves account takeover. The bank may choose to design a multi-factor authentication procedure that is useful not only in preventing fraudulent account openings, but is also applicable in authenticating customers to help prevent account takeover.

Financial Institutions as Trusted Authenticators

The idea that a bank may act as a trusted authenticator for its customers already has precedent for business customers. For example, Identrus is a company that has developed a global trust network among participating financial institutions. This trust network enables these banks to establish the identities of their corporate customers, and certifies them as trusted trading partners on the Internet. Businesses that previously had not dealt with each other now have a way of establishing trusted online relationships with each other. Another example is the Financial Agent Secure Transaction (FAST) project of the Financial Services Technology Consortium[10], which seeks to determine whether financial institutions can "leverage the relationships they have with both consumer and commercial customers to facilitate e-commerce by providing authentication, attribute information, or both."

Using one's bank as a trusted authenticator to prevent identity theft has several advantages. The creditor is not only relieved of the burden of directly contacting and authenticating the person named in an application, but is also relieved of responsibility for implementing the procedure. Now the creditor need only interact with an applicant's trusted authenticator via a standardized protocol. Furthermore, a bank is actually in a better position to authenticate one of its own customers than the creditor would be in trying to authenticate an applicant that it does not know. Presumably, the bank has

[10] See www.fstc.org

already verified the identity of its own customers, and has likely established a remote authentication procedure for purposes such as online (or telephone) banking.

Initial Signup and Authentication Procedures

The first step in the direct authentication procedure proposed here is the establishment of an initial signup and authentication process for use by trusted authenticators in creating a participant list. This procedure would be different than that proposed for PIDS. Each new participant would not need to contact a government agency and make a personal appearance before that agency. Instead, prospective participants would contact the bank where they already do business, and request that the bank act as their trusted authenticator. Or more likely, they would respond to a solicitation by the bank to participate in a new "identity theft prevention" program. When someone decides he/she wants to become a participant, the signup process is handled by the trusted authenticator, who is responsible for providing the necessary participant information to the list. Since the new participant is already an established customer of the trusted authenticator, the signup procedure should be relatively painless.

One of the provisions of the USA PATRIOT Act, enacted in 2001, is that banks must "know their customers" by verifying the identity of those customers. Imagine a scenario in which a potential identity thief wishes to open a new credit account in someone else's name. The thief knows, at minimum, the person's name and SSN. Since the participant list needs to be accessible online by creditors, it would not be impossible for the thief to determine whether his potential victim is a member of the list. Presumably the thief would be more likely to target individuals who are not on the list. In that case, the thief may simply decide to apply for a new account using the victim's personal information, figuring the risks would be minimal. Or, the thief might attempt to steal this person's identity by impersonating his victim and establishing an account in the victim's name at a financial institution that could then act as a trusted authenticator. However, this may be difficult for an imposter to do, in light of the PATRIOT Act.

Section 326 of the PATRIOT Act requires financial institutions to implement "reasonable procedures" to verify the identity of any person seeking to open an account. This has been interpreted by the Treasury Dept. as requiring that new customers provide a name, address, date of birth, and taxpayer ID number (e.g., a SSN or passport number)[11]. However, the methods used by banks to authenticate this information is crucial. The bank may simply require a new customer to produce a single photo ID. If an imposter can fraudulently obtain a photo ID with his picture on it, but with the personal information of his intended victim, then the imposter can defeat the system. As in the case of obtaining a driver's license, which has taken on the unintended role of a de-facto national ID card, it is critical that a person's identity be initially established with the trusted authenticator.

[11] JS-335, "Treasury and Federal Financial Regulators Issue Final Patriot Act Regulations on Customer Identification", US Dept of the Treasury, April 30, 2003

In an effort to reduce fraudulently obtained driver's licenses, the New Jersey Motor Vehicle Commission now requires a personal appearance by anyone renewing a driver's license. The person renewing the license must present a primary identity document such as a passport or birth certificate, plus at least one secondary document such as a social security card, old driver's license, health insurance card, etc. Banks may choose to adopt a similar one-time authentication procedure for verifying the identities of new customers that is based on information obtained from physical identity documentation presented in person, together with other "out-of-wallet" information provided by the customer. In addition to physical inspection of the identity documents, both types of information could be verified using information services offered by vendors such as Lexis-Nexis and others. Regardless of how it is done, a thorough initial authentication process further establishes the viability and appropriateness of financial institutions to act as trusted authenticators in preventing identity theft.

Liability and Business Considerations

Since participation would be voluntary on the part of individuals, the "trusted authenticator" approach to identity theft prevention would be most effective if it is well supported by most (if not all) financial institutions, and if large numbers of people choose to participate. It would be less effective in reducing the overall incidence of identity theft if it is attractive to only a select group of a bank's customers. Since there will be implementation costs involved with enabling financial institutions to act as trusted authenticators, these institutions will expect to realize some revenue as a result of providing such a capability. A bank might, therefore, position this authentication procedure as a new service that could be offered to its own customers. Initial participants might consist of a bank's "best" customers (if it is offered to them at no additional charge), or other customers most concerned about identity theft. Whether a bank would be able to generate much additional revenue from its own customers with such a service, however, is uncertain.

The business proposition for banks to act as trusted authenticators for their customers could also involve revenue generation from creditors who use this capability to authenticate applicants for new accounts. Recent changes to the Fair Credit Reporting Act contain a number of identity theft-related modifications that could influence this. One such modification involves the use of fraud alerts that consumers may place on their credit reports. Previously, creditors were not required to act on those fraud alerts. The new changes would require creditors to contact a consumer who has placed a fraud alert on his or her credit report (using a telephone number indicated in the alert), or to otherwise "take reasonable steps to verify the consumer's identity." These changes may provide greater incentive for creditors to rely on trusted authenticator services to aid in identity verification.

The issue of liability is trickier. As noted previously, it has been proposed that creditors making use of trusted authenticators for identity verification should be immune from liability for damages to identity theft victims if an account is mistakenly opened for an imposter. Assuming that the financial institutions, acting as trusted authenticators, adopt

uniform procedures for identity verification, they could provide a more reliable method of identity verification than simply requiring creditors to "take reasonable steps" to authenticate new account applicants whenever a fraud alert is noted on a credit report. Not only could the definition of "reasonable steps" vary between creditors, but fraud alerts themselves are usually attached to credit reports only after someone has already been an identity theft victim. However, if banks are to act as trusted authenticators, there is another liability issue to be addressed. Will trusted authenticators be liable to anyone if they make a "mistake?" Although this is an important (and unresolved) issue, the answer may depend, in part, on the nature of the response returned to a creditor seeking identity verification. A response that "guarantees" that the person named in a new account application is truly the person who applied for the account may entail a greater risk of liability than a response that simply reports on the reply the bank receives after contacting its customer ("yes, it really was me that applied for this account"). In any case, banks and other financial institutions may have strong reservations about acting as trusted authenticators if any liability at all is involved. The liability issue is one that probably needs to be addressed in any service agreements that financial institutions would have with other creditors in providing a trusted authenticator service. Liability issues could also be addressed in any new laws seeking to encourage direct authentication via trusted authenticators in performing identity verification.

Privacy Concerns

Individuals have become increasingly concerned and vocal about maintaining their privacy. Perhaps nothing best illustrates this more than the overwhelming response to the Federal Trade Commission's Do Not Call list. Regarding financial privacy, there is much debate about whether state governments should be allowed to enact stricter laws regarding financial privacy than federal laws allow, especially as regards the sharing of personal information among affiliated financial institutions. In the authentication procedure outlined in this paper, several privacy concerns may arise. The system implementing the authentication procedure will know which credit applications are being made in a participant's name. Most of these applications will be genuine, but some may be fraudulent. Should the system be allowed to keep permanent records of this information, and what type of privacy policies would apply to it?

Financial institutions acting as trusted authenticators will also possess that same information. Should that information be treated in the same way as other information the bank maintains about their customers? The Gramm-Leach-Bliley Act allows customers to opt-out of the sharing by banks of certain types of customer information with non-affiliated third parties, but does not allow such opting-out with regard to sharing with affiliates. Should the same rules apply to information obtained as a trusted authenticator? Perhaps an even greater issue concerns the handling of biometric information. As noted previously, financial institutions may choose to employ biometrics when authenticating their own customers. If biometrics are used, should biometric information provided to a bank by a customer be treated as strictly private information that cannot be shared without the express permission of the customer, or should it be subject to the looser privacy restrictions of Gramm-Leach-Bliley?

Financial institutions have generally resisted attempts to restrict sharing of customer information with others with whom they have business relationships. It could be argued that, in addition to a new service that banks could provide, the direct authentication procedure described here is also a kind of public service. As such, it's reasonable that any information gathered by financial institutions acting in the role of trusted authenticator should be subject to the strictest privacy protections. Financial institutions, if they are to maintain the trust of their customers and undertake this role on their behalf, must be sensitive to such concerns.

One result of both Prof. LoPucki's PIDS and the trusted authenticator approach to preventing identity theft is that the value of sensitive personal information in the hands of an identity thief becomes much less than before, since the simple possession of this information will be insufficient to open a new account in a victim's name. However, this does not suggest that laws aimed at restricting the use and availability of sensitive personal information are any less relevant. Such restrictions can still be valuable in helping to thwart identity theft for those individuals who are not participants. There are other privacy issues associated with the widespread availability of personal information, such as its use for marketing purposes, that such laws may address.

Technical Considerations

The "trusted authenticator" approach for authentication of credit applicants requires that creditors contact a list to determine if the person named in the application is a participant. If so, the creditor then requests that the participant's trusted authenticator provide some form of assurance to the creditor that the person submitting the application is the same person as is identified in the application. Although it is beyond the scope of this paper to delve into significant technical detail regarding the implementation of this scenario, a few points can be noted.

When the customer has indicated that the preferred mode of contact is email, it is very likely that the authentication procedure can be completely automated. When the preferred mode of contact is a voice phone call, it is likely that the authentication process would involve a human being who makes the call. However, this may not necessarily be the case in the future, as technologies such as Voice XML[12] and automatic speech recognition may be used to create an automated speech interface between an authentication system and the bank's customer.

The list of participants will not contain information needed to contact participants directly, but rather will contain a network address or some other pointer for the creditor to use in contacting the trusted authenticator. The creditor will send a standardized, secure message (conforming to some protocol) to the trusted authenticator that contains information about the person identified in the account application, as well some details about the type of account that is being applied for. Upon receiving the message, the trusted authenticator contacts its customer (the participant) to determine whether the

[12] See voicexml.org

credit application is legitimate, and then provides an appropriate response back to the creditor. This response might consist of an authorization to proceed (or not proceed) with the processing of the credit application, depending on the participant's response. Or, it might simply report on the participant's response. In either case, the creditor must trust that it is communicating with the proper trusted authenticator, and that the response it receives is genuine and not "spoofed." This requires some sort of trusted relationship to exist between the creditor and the trusted authenticator. However, a creditor will need to have trusted relationships with many different trusted authenticators, since participants will use many different authenticators. It is clearly infeasible to require each creditor to establish a separate trusted relationship with each possible authenticator.

One way this dilemma might be resolved is through "brokered trust" models between a creditor and the various trusted authenticators. Assume that the participant list is implemented by the financial services community. Further suppose that each financial institution that serves as a trusted authenticator itself has a trusted relationship with the entity maintaining the participant list. If a creditor establishes a trusted relationship with the entity maintaining the list for the purpose of determining if someone is on the list, the list entity now acts as a "trusted broker." The result is that the creditor has effectively established a trusted relationship with each of the trusted authenticators known to the list. The creditor, once it authenticates itself to the list (via a password, at minimum), can therefore be assured that the information it receives back from the trusted authenticator is genuine.

These brokered trust models involve concepts in identity management that are being specified by the Liberty Alliance in its Phase 2 specifications. The Liberty Alliance is a group representing more than 160 different organizations, including financial institutions, technology and security companies, service providers, and others. The goal of the Liberty Alliance is to develop open standards for federated identity and identity-based services. By "federated identity" is meant the linking together of identity information about a particular individual that is distributed across multiple domains. For the authentication procedure, the salient features of the Liberty (Phase 2) specifications pertain to implementation of the brokered trust model between creditors, the participant list, and the various trusted authenticators. A key component of the Liberty specifications that provides for this capability is the Security Assertion Markup Language (SAML), which is an XML-based specification for exchanging authentication and authorization information. In short, SAML could be used for the exchange of assertions (i.e., declarations of facts) between the creditor and the trusted authenticator pertaining to the authentication or authorization of the person attempting to open a new account in the name of a participant.

As previously noted, a trusted authenticator needs to contact its customer via email or telephone and verify the customer's identity before it asks about the pending credit application. At minimum, a two-factor authentication scheme will apply, since the customer has received a particular email or phone call at a pre-defined address (one factor), and will likely be asked to provide a password or PIN (the second factor). A third biometric factor could be added for increased security, if desired. One possible

reason for this is to strengthen the bank's means of authenticating its customers to prevent account takeover. When contact with the participant is via a voice call, a voice biometric (voiceprint) is the natural choice. A voice biometric is also advantageous in that the "liveness" of the customer can easily be verified. That is, to protect against the possibility that the customer's voice may have been previously recorded, the authentication mechanism may ask the customer to repeat a series of words or random digits, and verify the computed voiceprint for each word.

Biometrics for online authentication is a bit more problematic. Fingerprints would be the most likely biometric to use in an online session; however, attaching a finger scanner to one's computer would be expensive and burdensome. This is especially true for the more sophisticated finger scanners that attempt to ensure that the finger is "live" and is not simply a latex copy. Since computers do not come with built-in finger scanners, using finger scans for online authentication may turn out to be too costly. An alternative may be to integrate voice biometrics into the online authentication procedure. This might be done in two ways. Since many bank customers will have broadband Internet connections, a voiceprint could be obtained using a microphone connected to the computer and "voice-over-IP" for voice transmission to the authentication server. Another approach, which is currently supported by several vendors, would enable someone to provide a voiceprint by answering a phone call made by the authentication server to the person's landline phone, or cellphone, during the authentication process.

Conclusion

There is a natural tension between the ease with which people are able to access credit, and the degree to which the identities of those seeking credit are authenticated. The key is to establish authentication procedures that are least burdensome to creditors and their customers, while at the same time preventing the identities of unsuspecting consumers from being used to open fraudulent new accounts. Consumers who participate in direct authentication via a trusted authenticator may object to the idea that they will be contacted via email or a voice call for verification whenever they open a new account somewhere. But this shouldn't be a problem when new accounts are opened legitimately, since this will probably not occur very frequently. If a participant suddenly gets a flood of emails or phone calls requesting authentication, it's more likely that an identity theft is in progress. In that case, it is to the participant's advantage to be contacted, so that the theft can be prevented.

Financial institutions or creditors may object that requiring participants to be contacted will slow down the application process, or otherwise present a burden. There will almost certainly be some delay in the time required to process and open a new account. But this delay shouldn't be any longer, and could even be shorter, than would be experienced by creditors today when verifying a customer's identity in response to a fraud alert. For legitimate account openings, participants want the account to be opened, and will therefore be expecting the email or phone call requesting verification. In such cases, they will likely respond quickly. If participants are not expecting to be contacted, they will perhaps not respond as quickly, but those instances would more likely correspond to

fraudulent attempts to open an account. By acting as trusted authenticators, financial institutions strengthen their position as organizations that are concerned about protecting their customers from fraud. In addition, financial institutions become key players in the fight against identity theft, and can help creditors to reduce their losses to identity theft as well.

In order to implement this proposal, changes to current laws will be required. These are essentially the same changes described by Prof. LoPucki. The most fundamental change would be to prevent the simple knowledge of a person's SSN from acting as a "password" to authenticate that person's identity. Since it is not difficult to discover the SSN of an individual, this change seems long overdue. A second change would be to encourage creditors to authenticate the identities of applicants for new accounts according to some minimal standards, such as following the procedures outlined here. Failure to do so would render the creditor liable for damages should a new account be opened for someone who has appropriated another person's identity. Third, other laws aimed at maintaining financial privacy by restricting the use or distribution of personal information for purposes such as marketing should not be affected.

Acknowledgements

The author would like to thank Carol Coye Benson, Linda Foley, Mike Thibodeaux, Richard Parry, and Jim Salters for their helpful comments on an earlier draft of this paper.

About the Author

Robert Pinheiro (bp@bobpinheiro.com) is an independent security researcher interested in authentication technologies, identity management, and secure electronic commerce. He earned the SANS GIAC Security Essentials certification (GSEC), for which he submitted a research paper entitled "Strong User Authentication For Electronic and Mobile Commerce." He has over 20 years experience in the telecommunications industry, where he worked as a research scientist and systems engineer at Telcordia Technologies (formerly Bell Communications Research) and Bell Laboratories. His work involved Internet telephony (Voice Over IP), Intelligent Networks, Digital Subscriber Lines (DSL), Integrated Services Digital Networks (ISDN), secure electronic commerce, and software agent technology. He has an MS in Statistics from Rutgers University, and an MS in Applied Mathematics from Polytechnic Institute of New York (now Polytechnic University).