

A Proposal For Using Authentication Services Provided By Financial Institutions In The Prevention of Identity Theft

Bob Pinheiro
Robert Pinheiro Consulting LLC
bp@bobpinheiro.com

Introduction

As banks begin implementing stronger forms of authentication for access to online banking accounts in response to the recent FFIEC Guidance, NACHA is exploring possible ways that these authentication technologies can be leveraged for other purposes. NACHA will be evaluating one such concept in 2007 as it tests a “Credit Push” model for online payment. The development of business cases for other possible applications that make use of emerging strong authentication capabilities is also being considered as part of NACHA’s goal of a common framework for online financial services. High among possible applications is an authentication-only service that can be provided to third parties. We propose here another version of such a service: an authentication-only service that can help to prevent identity theft. *It should be noted that the ideas expressed here are speculative and meant to stimulate discussion and debate about the feasibility of using strong authentication methods in the fight against identity theft.* NACHA may wish to further investigate these concepts as it develops business cases for authentication-only services provided by financial institutions¹.

New Banking Services That Leverage Strong Authentication

Credit Push is a more secure way for customers to pay for online purchases directly from their bank accounts. Without Credit Push, paying for online purchases directly from a bank account by providing an account number and bank routing number to an online merchant is very risky, because anyone who knows that information can siphon money out of the account without much difficulty. The problem is that the ACH network that handles these electronic payment transactions has no built-in way to verify that the person initiating an electronic debit from a particular bank account is actually authorized to do so. To address this deficiency, Credit Push requires that consumers wishing to pay for an online purchase by directly debiting their bank account must authenticate themselves to their bank as part of the payment process. This establishes their authority to access the account, and to make payments from it. After the customer is authenticated, the customer’s bank makes a direct transfer of funds to the merchant’s bank. By introducing authentication procedures into the payment process, the possibility of fraudulent debits from the customer’s account is significantly reduced.

¹ We will use the term “bank” to refer to such institutions, since the FFIEC guidance applies more specifically to banks rather than financial institutions in general. This is not meant to preclude the possibility that other types of financial institutions could offer the services proposed here.

Another possibility for leveraging a bank's strong authentication capabilities is to provide an authentication-only service to third parties. One version of such a service has already been tested as part of the federal government's E-Authentication initiative. The idea is that government agencies that conduct business with the general public want to encourage people to conduct these transactions online, rather than in-person, over the phone, or via "snail mail." An example would be a request to change an address for Social Security purposes. But before honoring such a request, the government agency must verify the identity of the person requesting the service. As with Credit Push, a bank that has deployed strong authentication for online banking could verify whether anyone claiming the identity of one of its customers for the purposes of a government service is truly that person. After the authentication is performed, the bank would then notify the government agency of the result via an electronic identity-related assertion message.

Preventing Identity Theft Using Strong Authentication

A bank's strong authentication capabilities could also be used to help prevent any of its online banking customers from becoming victims of identity theft. In this application of strong authentication, the bank acts as a trusted third party that asserts to a relying party whether or not a given individual is able to satisfactorily authenticate to the bank for access to online banking services associated with the person whose identity is claimed.

For the purposes of this discussion, identity theft is defined as using another person's identity-related information to open a new credit account. Identity theft is enabled by the widespread business practice that accepts as "proof" of someone's identity the fact that a person may know certain information about another person that is not truly "secret", such as a social security number, birthdate, or mother's maiden name. Because of the recent introduction of breach notification laws, the nation has become aware that large amounts of sensitive personal information maintained by businesses, government agencies, and other organizations seem to be routinely lost or stolen. Although better information security can certainly help to prevent identity theft, the widespread availability and distribution of this information suggests that any viable solutions to the identity theft problem must include ways to make knowledge of stolen personal information, by itself, insufficient to commit identity theft. An obvious way to do this could require a "stronger" form of identity authentication, for people opening new accounts, that relies on other factors besides knowledge of personal information.

Today, it's easy for a fraudster who obtains personal information about someone to be able to commit identity theft, because a creditor establishing a new account for someone typically make only a minimal, if any, attempt to verify the identities of new account applicants. Indeed, since the person applying for the account typically will not have a prior relationship with the creditor, in most cases the only way for the creditor to verify an applicant's identity is to physically inspect identity documents when the application is made in-person, or to resort to a knowledge-based authentication service from a trusted data source when the application is made online. But because of the added cost, time, and inconvenience involved, knowledge-based authentication is not usually performed for accounts opened online. Instead, if the identity information provided by the applicant

generally matches the information contained in a credit report, it's assumed that the applicant's identity has been verified.

The financial services industry, possibly through a newly-created industry consortium, could offer an identity theft prevention service to customers of participating banks, as well as an authentication-only service to creditors for verifying the identities of new account applicants. As with Credit Push and E-Authentication, the service would leverage a participating bank's strong authentication capabilities already in use for online banking. Customers of participating banks would be invited to register for this service, and if the customer chooses to register, anyone henceforth claiming that customer's identity when opening a new credit account would be subject to the same strong authentication procedure used for access to online banking.

In the case of new account applications being made online, the service might work as follows:

1. Someone wishing to open a new credit account provides identity information (Name, SSN, birthdate, etc.) at the creditor's website as part of the new account application process.
2. If the identity information corresponds to someone who is participating in an identity theft prevention service, the applicant will be redirected (at some point during the account opening process) to a secure webpage that will take the applicant through the identity authentication procedure.
3. The authentication procedure will be the same layered, risk-based, or multifactor authentication procedure that the person whose identity is being used to open the account would need to undergo for accessing online banking services at the bank where that person is registered. The result of the authentication procedure will be provided to the creditor in the form of an identity-related assertion message from the authenticating bank.
4. If the authentication fails, the creditor will assume that the credit application is fraudulent and will not open an account. If the authentication is successful, the creditor then proceeds to verify that the applicant, whose identity has now been verified, is credit-worthy by checking the applicant's credit report.
5. If the applicant is credit-worthy, a new account is opened.

If the applicant is applying in-person, the person who is actually entering the applicant's information into a computerized application process will be prompted at some point to ask the applicant to sit in front of the computer and go through the authentication process.

Is This Practical and Effective?

For the authentication service just described to be practical and effective, several issues must be addressed.

- Identity thieves who steal personal information and seek to open new accounts using this information must go through the authentication procedure if the person whose

information is stolen has registered for the service. The account applicant cannot decide, during the account opening process, whether or not authentication is invoked. To allow an applicant to bypass the authentication process would defeat the purpose of the service and make identity theft possible.

- There must be some way to determine, during the account opening process, whether the identity being used to open the account has been registered for the identity theft prevention service with some bank. How this might be done is beyond the scope of this note; however, several possibilities are suggested below:
 - a. The most obvious possibility is to present a huge pull-down menu listing all the banks that offer identity theft prevention services. The applicant would need to pick the bank where he/she is registered². While this possibility would seem to make identity theft more difficult, since a fraudulent applicant would need to know at which bank his victim is registered, this approach seems very unwieldy. There are probably many banks with similar sounding names, and legitimate applicants might become too confused.
 - b. Another possibility is that a federated network of banking servers might be developed, based on Liberty Alliance (or other) specifications. An applicant's Social Security Number, for example, might be encrypted and submitted to this federated network, where the encrypted SSN could be matched against some type of database that would contain a pointer to a server associated with the bank where the "owner" of the Social Security Number is registered.
 - c. A third possibility is that existing networks that banks and creditors already use, such as credit card networks, might somehow be adaptable and usable for this purpose.
- An identity thief in possession of someone else's identity information, and seeking to open an account using that identity, should not be presented with an authentication webpage that identifies the victim's bank. Doing so would further expose the victim to the identity thief.
- The authentication procedure used for the identity theft prevention service, which is the same as used for a participant's online banking, would need to be able to accommodate a situation where the participant is applying for a new account (such as a car loan) in-person at the creditor's office. This implies that one of two things must be true:
 - EITHER the authentication procedure must not rely strictly on the necessity of authenticating from a particular computer or other device that may not be in the possession of the participant when traveling,
 - OR authentication must take place at a later time when the participant is in possession of the hardware devices necessary to perform the authentication.
- Many bank accounts are joint accounts with a spouse or other person. Typically, a bank doesn't issue separate login IDs or passwords for use by different people

² We can assume that a person is registered for the identity theft protection service with only one bank, which acts as the person's "trusted authenticator."

authorized to access the same account. Reliance on an ability to authenticate to such accounts for identity theft prevention purposes may mean that the authentication procedure needs to be able to distinguish between these joint owners. One option is to consider the role of biometrics as unique “authenticifiers” for different individuals.

- Since the creditor will need to trust an identity-related assertion received from a bank that the creditor may not necessarily have a relationship with, there needs to be a trust relationship between that creditor and the bank. This may involve the establishment of “trust frameworks” or “circles of trust” as envisioned by groups such as the Electronic Authentication Partnership and/or Liberty Alliance, respectively.
- In response to the FFIEC Guidance, banks are considering several types of authentication options, including risk-based authentication in addition to multifactor authentication. The upshot is that the type of authentication that a bank may use for initial account access may be “weaker” than the authentication required for high-risk transactions that move large amounts of money out of a customer’s account. It needs to be determined whether the “assurance level” of the authentication mechanism that would be invoked as part of an identity theft protection service is sufficient to verify a claimed identity with a sufficient degree of certainty.
- There needs to be sufficient incentive for creditors to verify the identities of those seeking to open new accounts. Identity verification may involve additional costs to the creditor. Besides the general desire to avoid opening fraudulent accounts, there may evolve a legal liability to identity theft victims if creditors do not take “reasonable” steps to verify identities before opening new accounts. Another possibility is that the creditor’s bank may provide some additional incentive to the creditor to avoid fraudulent new accounts. A final possibility is that some type of collaboration between the banking industry and the credit bureaus may result in a single service that provides identity verification as well as credit scoring functions.
- Liability issues always seem to present a roadblock to the viability of an authentication service. Yet banks provide signature guarantees for their customers, and notary publics provide a similar type of service. The difference seems to be that notary and signature guarantees require that someone appear in person and present physical identity credentials, whereas in the case of an online authentication service, that is not the case. Yet if banks begin to implement strong authentication for online banking purposes at a high assurance level, the additional strength of the authentication procedure ought to make it comparable to someone appearing in person.

Is There A Business Case?

A business case for this particular application of a bank’s strong authentication capabilities obviously requires that sufficient revenue can be generated by the service. Following are a few ways that revenue might be generated.

- Banks may offer an identity theft prevention service to their customers for a nominal subscription fee. As such, the willingness to pay for such a service may be similar to the willingness to pay for other identity theft “prevention” services that individuals may use, such as credit monitoring services offered by credit bureaus. However, because the bank service actually does prevent identity theft, whereas a credit monitoring service merely notifies one of changes to a credit report, it’s possible that the willingness-to-pay for an identity theft prevention service may be higher than for a credit monitoring service from a credit bureau.
- Banks may derive revenue directly from the creditor in return for an authentication service that helps the creditor to ensure that the new account is legitimate. Since creditors are already paying the credit bureaus a fee for checking credit reports, the additional fee could be viewed as an additional incremental cost.
- Banks and credit bureaus may decide to jointly offer a service to creditors that, for a single fee, could provide both a credit check and an identity check.
- Some credit bureaus, in response to various state laws, are offering “security freeze” services that allow consumers to prevent access to their credit files unless specifically authorized by the consumer. These security freeze services must provide consumers the ability to temporarily lift a freeze, should they wish to apply for credit themselves. However, the method that credit bureaus typically use to determine if a legitimate consumer wishes to lift a security freeze depends on knowledge of a Personal Identification Number (PIN). To steal the identity of someone with a security freeze, then, identity thieves would simply need to refocus their information-stealing activities towards obtaining these PINs. This situation presents an opportunity for banks to provide strong authentication services to credit bureaus for the secure lifting of a security freeze.

Comments

Comments are invited. Please e-mail the author at bp@bobpinheiro.com.