The Basics of Authentication in the ACH Network

Contributors: *Susan Pandy, Nacha; Peter Tapling, Authentify; Audrey Touma, Chase Paymentech; Susan Doyle, Commerce Bank; and Ron Paradiso, Nelnet Solutions*

The objective for this resource is to help ACH Network participants better understand authentication technologies that are available in the marketplace. Authentication methods and tools help the Originator to verify the identity of the customer who is authorizing the debit to his or her bank account, and help the ODFI to verify the identity of the corporate customer who is originating these debits. This is a common challenge among ACH Network participants. No authentication technology alone is a solution and ACH Network participants should understand that the approach chosen should be part of their business' overall risk management strategy. The best approach is a layered one that combines several technology solutions, because each solution has its own element of risk and is dependent on the nature of the business model it supports.

The technologies addressed in this resource are not exhaustive and Nacha does not endorse the use or application of any one particular technology.

Why Does An Originator Have to Use Commercially Reasonable Authentication Methods?

The Nacha Operating Rules use the terminology, "Verification of the Identity of the Receiver" to refer to the requirement that ODFIs warrant that their WEB Originators are using commercially reasonable methods of authentication to verify the identity of their Receivers. ODFIs sometimes ask what constitutes "commercially reasonable" authentication methods for this purpose. According to the Nacha Operating Rules, "a commercially reasonable system, technology, practice, or procedure is one that corresponds to the commonly accepted commercial practices among similar types of transactions. The concept of commercial reasonableness means that a party, given the facts of a specific transaction, acted in a way that other similar parties would have acted" (OG 25). A similar standard is used in Article 4A of the Uniform Commercial Code (UCC) with respect to allocation of liability between ODFIs and senders (Originators of ACH credits).

There is no single industry standard for verification of the identity of the Receiver. The authentication process for WEB transactions can consist of two steps:

1. Ensuring that the name given for a particular transaction corresponds to a real-world identity, and
2. Confirmation that the person providing that name is truly the Receiver associated with an account and not an unscrupulous impersonator.

The combination of increased identity theft, fraud (which affects both the merchant and customer), and focus on terrorism prevention has heightened interest for deploying stronger authentication methods.

Authentication is an important component of managing the risk for WEB payments. The anonymous nature of the Internet creates significant challenges in the verification process, since traditional methods of verification typically used in a face-to-face setting are not viable on the Internet (e.g., photo ID). Since Originators may ultimately be responsible for transactions that are returned as unauthorized, it is to their benefit to incorporate adequate levels of authentication into their business practices.

Furthermore, a risk-based approach to authentication allows a business to take into account the specific circumstances of the transaction, i.e. the type of transaction, the type of customer, etc. For instance, recurring transactions that are enabled for regular bill payment transactions with known customers may require less robust authentication than one-time payments made from new customers.

A risk-based authentication model helps to prevent a bad user experience, too. Some businesses may be employing too many authentication tools for activity that may be low risk. Therefore, it is important for businesses to evaluate their overall need for authentication tools and solutions.

Why Does An ODFI Have to Use Commercially Reasonable Authentication Methods?

It is equally important for ODFIs to employ commercially reasonable authentication methods to identify its customer when enabling ACH credits to be sent directly from its accounts. The Federal Financial Institutions Examination Council (FFIEC) guidance, "Authentication in an Internet Banking Environment," was originally issued in 2005 and updated in June 2011 (2011 Supplement). The FFIEC determined that the use of single factor authentication methods, such as passwords and user identification, are no longer sufficient if an electronic banking system permits high-risk transactions (i.e., movement of funds or access to customer information). The FFIEC concluded that financial institutions should implement multifactor authentication, layered security or other controls reasonably calculated to mitigate the risks.

The 2011 Supplement is a critical key to understanding trends in what is considered "commercially reasonable" authentication technology and for understanding the bank regulators' expectations for such controls. As payments technology and services have evolved, so too have the internal and external threats to those services, as well as the understanding of what may be a commercially reasonable method for addressing those ever-changing threats. An example of how the commercially reasonable standard has changed over time is indicated by the shift away from the use of username and passwords as the only means of authentication, to the declaration that this practice is no longer considered sufficient by the FFIEC. The 2011 Supplement also points out that simple device ID and challenge questions are no longer considered effective as primary controls and that additional controls are required, thereby underscoring the need for a layered approach to security. As indicated by the 2011 Supplement, threats may eventually evolve to the point that technologies and methods that were once acceptable may be no longer be considered commercially reasonable for various types of transactions.

To further understand the concept of what it means for authentication methods to be commercially reasonable, readers may wish to consult the recent court case, PATCO Construction Company, Inc. v. Ocean Bank (now People's United Bank) (No. 11-2031). The trial court's original ruling in May 2011 favored the bank and its online security procedures. However, this ruling was reversed in July by the U.S. federal appeals court for the First Circuit, which ruled that Ocean Bank's security procedures were "commercially unreasonable" for purposes of UCC Article 4A's requirement that banks offer commercially reasonable security procedures to their customers in order to avoid liability for certain unauthorized transactions.

The case involves the plaintiff, PATCO, a Maine-based construction firm, which was negatively impacted by a series of fraudulent transactions from the firm's commercial account with the former Ocean Bank. PATCO claimed that Ocean Bank was not in compliance with the existing FFIEC authentication requirements and did not act in a commercially reasonable manner when it relied solely on login and password credentials and universally applied challenge questions to verify transactions.

In the court's review of the bank's security measures, it noted that several security measures were available and used by others but were not employed by Ocean Bank, including out-of-band authentication, user-selected picture functions, tokens, and monitoring. Token batteries can last 3-5 years and the devices cost anywhere from $5 - $50 depending upon size, sophistication, features, order quantity, etc. Tokens also include an installation cost on the merchant's server, accompanied by an internal resource to provide maintenance and oversight. Depending on the size and complexity of an institution's systems, the cost of even a single account takeover and/or fraudulent wire transfer may considerably outweigh the investment.

In addition, because Ocean Bank effectively required that all transactions over $1 be approved using challenge questions, the court concluded that the bank had substantially increased the risk that the answers to those questions would be intercepted, thereby lessening the effectiveness of that authentication method. Further contributing to the court's conclusion that the bank's security systems were unreasonable was the fact that Ocean Bank's transaction-monitoring practices were inadequate and its lack of standardization for customer notification when high-risk transactions were detected. Although no one failure was necessarily fatal, as a result of the combination of all these factors, the court concluded that Ocean Bank's deficient "one-size-fits-all" approach to monitoring and authenticating high-dollar transactions unreasonably exposed PATCO to more risk.

For more information about this case see:

http://www.bankinfosecurity.com/inside-patco-fraud-ruling-a-4927/op-1

http://docs.ismgcorp.com/files/external/First_Circuit_Order_070312.PDF

http://www.bankinfosecurity.com/ach-case-headed-to-trial-a-2912

Why is Understanding Authentication Important?

Regardless of whether other courts follow the PATCO case in the future, it underscores the critical nature of understanding the importance of authentication as part of an overall risk management strategy. To mitigate fraud risk within the ACH, it is important for an ODFI to employ commercially reasonable authentication methods, and for the ODFI to ensure that its Originator is employing commercially reasonable methods to verify the identity of the Receiver. While the Nacha Operating Rules require WEB Originators to deploy commercially reasonable procedures to verify the identity of the consumer, it is the ODFI that is ultimately responsible for the transaction. The ODFI will likely be considered a source for advice in selecting an identity verification method by the Originator. ODFIs are encouraged to work with WEB Originators to develop sound methods to verify the identity of the Receiver.

The following section discusses some of the methods that are available for satisfying authentication needs. In order to satisfy authentication requirements, ODFIs may wish to consider utilizing a combination of the following methods based on their overall risk management strategy. Nacha does not endorse any specific technology or approach, as each ODFI must consider which technologies, processes and procedures are most appropriate for managing risk.

Authentication Technologies

Device Identification

Simple Device Identification (Device ID): This method typically uses a cookie loaded on the customer's PC to confirm that it is the same PC that was enrolled by the customer and matches the logon ID and password that is being provided. However, experience has shown this type of cookie may be copied and moved to a fraudster's PC, allowing the fraudster to impersonate the legitimate customer. Device ID has also been implemented using geo-location or Internet protocol (IP) address matching. However, increasing evidence has shown that fraudsters often use proxies, which allow them to hide their actual location and pretend to be the legitimate user.

Complex Device Identification (ID): A technique which uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics including PC configuration, IP address, geo-location, and other factors. Although no device authentication method can mitigate all threats, the bank regulatory agencies (FFIEC 2011) consider complex device ID to be more secure and preferable to simple device ID. They further indicate that "[i]nstitutions should no longer consider simple device ID, as a primary control, to be an effective risk mitigation technique." (FFIEC 2011 Supplement to Guidance on Internet Banking Authentication)

IP address matching and geo-location techniques are methods used to implement device ID.

IP Address/Geo-Location

Geolocation is the practice of determining the physical, real world location of a person, device or subject matter using digital information processed through the Internet or other electronic means of communication. A growing trend in geolocation is deriving the city, ZIP code or region from which a person is or has connected to the World Wide Web by using their device's IP address or that of a wireless access point, such as those offered by coffee houses. Another form of geolocation involves utilizing the exact location featured in photo or video content based on longitude and latitude coordinates attached digitally to the media file manually or by GPS-enabled cameras. Even when not precise, geolocation can place users in a bordering or nearby city, which may be good enough for the entity seeking the information. This happens because a common method for geolocating a device is referencing its IP address against similar IP addresses with already known locations.

Tokens

A token, or security token, assists in the identification of a user of computer services. The token is a physical device, normally the size of a thumb. The range of tokens include the most popular that you can attach to your key chain (disconnected tokens) to actual flash drives (USB – connected tokens).

An example using a disconnected token would begin during an online login session with the user being prompted to depress a button that generates a random number that can be key entered onto the screen. The token generates an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and a factory-encoded random key (known as the "seed"). The seed is different for each token, and the command seed is also loaded into the corresponding server at the merchant. Most login sessions also require an additional factor (multi-factor authentication) like a PIN or password to be key entered as well. The token may also return a follow-up token number which should match the number returned on the screen by the bank or merchant.

Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods. Commercial solutions are provided by a variety of vendors, each with their own proprietary (and often patented) implementation of variously used security features. In today's environment, many banks require their commercial client users to use tokens to authenticate into online banking. However, it should be noted that tokens are at risk to man-in-the-middle (MITM) attacks.[1]

Tokenization of data is another valuable method of protection; however, it is outside the scope of this resource and will be discussed in a future resource related to the uses of encryption.

ID Verification Check

ID verification is a method that takes into account a number of personal attributes about an individual in order to verify their identity. For instance, certain attributes may indicate some type of suspicious or fraudulent activity in real-time when compared to database intelligence (i.e. the address is linked to 75 different names).

ID verification occurs when a consumer is at the checkout area of a merchant's website. As part of the checkout process the consumer is requested to provide some personal information in addition to bank account information (name, address, phone, email, etc.). Once the consumer has provided their personal data and clicks the submit button, a real time transaction is launched to the ID verification provider. The information is compared against a number of positive and negative databases and within milliseconds provides an ID score back to the merchant.

This score can reflect a variety of information such as:

1. The personal information is found to be a good or bad match based on real-time and historical records, and
2. The level of any other suspicious activity occurring that is related to any of the individual components of personal information provided.

Based on the ID score, the merchant can choose to allow the consumer to proceed to the next step and complete the transaction, terminate the transaction, or temporarily put the order on hold in order to conduct further investigation.

Depending on which ID verification provider a merchant or business is working with, the merchant can collect a wide range of personal information from the consumer in order to perform a real-time ID check. A combination of some of the following personal attributes used in this process include: name, current and/or former address, phone number, email, SSN, DOB, and shipping address.

Identity verification is an effective way to help merchants and businesses mitigate risk early on in their payment process and relationship with a consumer. Numerous providers who offer a broad range of services are available to businesses of all sizes.

Knowledge-Based Authentication

Knowledge-based authentication (KBA) is a method of authentication which seeks to prove the identity of someone seeking to access a service, such as a website. As the name suggests, KBA requires the knowledge of personal information of the individual to grant access to the protected material. There are two types of KBA: "static KBA", which is based on a pre-agreed set of "shared secrets"; and "dynamic KBA", which is based on questions generated from a wider base of personal information.

Static KBA (Shared Secrets): Static KBA, or "shared secrets" or "shared secret questions", is commonly used by banks, financial services companies and e-mail providers to prove the identity of the customer before allowing account access, or in the event that a user forgets their password. Upon initial contact with a customer, a business using static KBA must collect the information to be shared between the provider and customer, most commonly the question(s) and corresponding answer(s). This data must then be stored, only to be retrieved when the customer comes back to access the account. The weakness of static KBA was demonstrated in an incident in 2008 where unauthorized access was gained to the email account of former Alaska Governor Sarah Palin. The Yahoo! account's password could be reset using shared secret questions, including "where did you meet your spouse?" along with the date of birth and zip code of the former governor, to which answers were easily available online.

Some identity verification providers have recently introduced secret sounds and/or secret pictures in an effort to help secure sites and information. These tactics require the same methods of data storage and retrieval as secret questions.

Dynamic KBA: Dynamic KBA is a high level of verification that also uses knowledge questions to verify each individual identity, but requires no previous contact. This is because the questions are generated spontaneously based information in a consumer's personal aggregated data file (public records), compiled marketing data, or credit report. To initiate the process, basic identification factors, such as name, address and date of birth must be provided by the consumer. Then questions are generated in real-time from the data records corresponding to the individual identity provided. Typically the knowledge needed to answer the questions generated is not held in a wallet (some

companies call them "out-of-wallet questions"), making it difficult for anyone other than the actual consumer to know the answer and obtain access to secured information.

Dynamic KBA is employed in several different industries to verify the identities of customers as a means of fraud prevention and compliance adherence. Because this type of KBA is not based on an existing relationship with a consumer, it gives businesses a way to have higher identity assurance on customer identity during account origination.

Voice Recognition Authentication

Voice biometric authentication is the use of a customer's unique vocal characteristics to verify the identity of the individual. It is becoming a more widely deployed form of biometric authentication because voice samples can be captured via telephone with no requirement to distribute any special purpose hardware to users.

Voice biometrics work by capturing a speech sample from the customer in a trusted manner and creating a baseline voice "print." Once that print has been established, the next time the customer calls in (or is called), they simply have to provide another speech sample and the software will create a new print to compare with the baseline print.

The cost of deploying voice biometric authentication has come down as the technology has matured, and the capability can now be purchased as a "pay for use" service. It is quite common now to see voice recognition software being used in call centers.

It should be noted that all biometrics are statistically modeled, therefore, the results are based on significance levels versus binary "yes" or "no" results. Biometrics are not a silver bullet solution to protect against fraud and biometric authentication can be subject to various intentional attacks. For example, a voice sample for a given user can be captured and used by fraudsters. While the voice and other biometric vendors proclaim their security, time has shown that criminals will find ways to overcome the system security. These limitations should be considered when designing the overall risk management strategy which will include use of biometric authentication.

Out-of-Band Authentication

Out of Band Authentication (OOBA) is the use of a network connection to confirm a transaction which is different from the network connection on which the customer may have initiated a transaction. For example, when a customer initiates a transaction on a website, the bank will automatically place a telephone call or send a text message to the customer. The customer may confirm the details and then exchange a unique transaction code between the telephone and website in order to complete the transaction.

OOBA has proven successful in defeating broad based Man-In-The-Middle (MITM) and Man-In-The-Browser attacks (MITB). OOBA has grown in popularity because it does not require any new hardware or software to be distributed to customers and customers require no training to use the system.

Most fraudsters don't possess the technical sophistication to hijack text messages or operate a MITB Trojan; and even those that do must invest a lot of resources in order to complete a transaction secured with OOBA. Therefore, it is not surprising that when possible, fraudsters try going around OOBA by taking advantage of the enrollment process for OOBA (to get a telephone number they control into the profile for the user) or to intentionally fail the OOBA process and try to beat the failover process.

For OOBA to be most effective, the enrollment processes must ensure that the person opting-in to the service is the legitimate customer and not a fraudster. Asking personal questions that cannot be easily obtained through phishing, keylogging or background checks (see "Dynamic KBA" above) during the enrollment process will help authenticate the user and make OOBA that much more effective.

For OOBA to work well, the bank must have the customer's accurate phone number(s) on file and protect those telephone numbers. If not, come the day of the transfer the customer will not be able to receive the transaction code and complete the transaction. The enrollment for this service is often done online and if it does not incorporate tough authentication questions, will leave an opening for the fraudster.

It should also be noted that malware exists for mobile phones which can intercept or reroute SMS messages, so additional risk mitigation steps should be taken if OOBA via SMS is employed. OOBA has become so popular that there has been an increase in underground "SMS forwarder" services offered to fraudsters. These services offer phone numbers from all over the world that would immediately forward any text message to the fraudster's phone– streamlining the process of obtaining a local number (you don't want to provide a US bank with a Russian phone number) to accept transaction authentication codes sent by the banks.

As with the authentication approaches outlined here, OOBA is not bulletproof but it is an effective tool as part of a broader layered approach to keep fraudsters at bay. Design of the overall customer experience has a very big part of whether OOBA succeeds or fails.

Eventually, when the routes used to bypass security measures are themselves secured, most fraudsters will have no choice but to circumvent the problem in a different way — by targeting someone else. Source: http://www.securityweek.com/out-band-authentication-how-fraudsters-circumvent-sophisticated-security-measures.

---

[1] "Man-in-the-Middle" attacks refer to a hacking technique whereby the criminal intercepts communications between two systems and thereby is able to gain control over those communications.