Retail Payments Risk Forum
A CATALYST FOR COLLABORATION

# IMPROVING CUSTOMER AUTHENTICATION

**David Lott, Payments Risk Expert**

Retail Payments Risk Forum Working Paper
Federal Reserve Bank of Atlanta
April 2015

**Abstract:** Authenticating the parties in a payment transaction efficiently and with a high level of confidence is critical to the ongoing safety and soundness of our payment system. As technology has led to new forms of payments and the use of remote payment channels, there has been a growing challenge to modify existing and develop new authentication methods that deliver the necessary levels of efficiency and confidence. This paper examines the evolution of customer authentication methods from the early days of visual identification to the present environment of using physical and behavioral characteristics, known as biometrics. While the authentication of the payment order itself is separate from the authentication of the parties to a payment transaction, the separation of the two can be difficult in various payment instruments. The paper takes a high-level look at the authentication issue from a legal and regulatory viewpoint. Each of the authentication methods are reviewed as to their process, advantages and disadvantages, and applicability to the payments environment. Identification processes have the potential to create conflicts with an individual's privacy rights, and this conflict is examined. Finally, the paper closes by discussing the key learnings obtained from this research effort.

The paper is intended for informational purposes and the views expressed in this paper are those of the author and do not necessarily reflect those of the Federal Reserve Bank of Atlanta or the Federal Reserve System.

# IMPROVING CUSTOMER AUTHENTICATION

## TABLE OF CONTENTS

# Working Paper:

# Improving Customer Authentication

In early 2013, the Retail Payments Risk Forum (RPRF) team identified authentication as a critical element in the security of payment systems. The team divided the payment authentication issue into three distinct phases: 1) authentication of the customer/device to access an account and the ability to perform transactions, 2) authentication of the transaction during processing, and 3) secure storage of the authentic transaction record after the transaction has been completed. While this paper focuses on the first phase of authentication, reviewing methods used to authenticate the user and the payment form factor, discussion of the authentication of the payment itself will take place from time to time as separating the two stages can be difficult for some payment forms.

The RPRF held a forum at the Federal Reserve Bank of Atlanta in July 2013 on the topic of improving customer authentication. A link to the event can be found here. Keynote speakers and discussion panels provided the audience of regulators, law enforcement, bankers, merchants, and transaction processors with a wide range of information and suggestions as to how to make the payment ecosystem safer. A summary of the forum's proceedings can also be found on the website noted earlier.

Using the information provided at that forum as a foundation and supplementing with additional research, this paper incorporates the RPRF's continuing efforts of research and discussions with payment security leaders on the topic of improving customer authentication. Since the payments environment is a dynamic one with new payment form factors (such as mobile phones) being introduced and new criminal attack vectors cropping up, our effort is in the form of a working paper with the expectation of providing updates as the payments ecosystem evolves and new customer authentication technologies and processes emerge and mature.

## Background

It is important to define the term *authentication* and show how it is distinct from the word *authorization*. The two terms are sometimes interchanged because the two events often occur together, but such usage is incorrect as they are two distinct concepts. Authentication is a process used to verify the identity of the party, basically using different types of credentials to prove the person is who they claim to be. On the other hand, authorization is the association of that identity with certain rights and privileges. For example, a teller can use a driver's license to verify the identity of the person standing at the teller's window (authentication). Once the person is verified, the teller then has to ensure that the person is authorized to conduct the desired transaction on the affected account.

In the electronic transaction world, the authentication and authorization processes happen almost simultaneously. Once the teller has successfully entered a user ID and password, the teller is shown an online banking tool that has already been configured to provide a listing of accounts that the customer is authorized to use. This tool also indicates the types of transactions the customer is authorized to perform.

User authentication is a concept that is as old as humankind. The first methods of authentication were generally based on the unique physical characteristics of the person, such as facial appearance or voice. This method worked well when there were small, isolated communities and everyone knew each other. As commerce expanded outside of these villages where business transactions had been conducted in face-to-face meetings by people who knew each other, the need for other authentication methods grew. Since the vast majority of the population were not literate, was seals or other types of imprinting devices were often used along with a signature to help support authenticity, but the method wasn't foolproof. One of the first written records of authentication fraud comes in the Old Testament. Queen Jezebel forged her the signature of her husband, King Ahab, on a letter, which led to the king's confiscating a vineyard.[1] In the days of the ancient Roman Empire, the position of a notary public was developed[2] to serve as a representative appointed by the government to authenticate people and witness the execution of certain legal documents.

In the late 19th century, Alphonse Bertillon, a French police officer, developed the Bertillon System, which used measurements of a number of a prisoner's physical features (such as middle finger length, foot size, head length and width, eye color) along with a frontal and profile photograph to provide what was thought to be a unique set of identifiers to help police track suspects. While other aspects of Bertillon's work in establishing principles for documenting crime scenes and victims are still used today, the body measurement system was found to be flawed in the early 1900s. Two inmates at Leavenworth Prison in Kentucky with similar names were found to have the same physical measurements—so they could not be distinguished from one another on the basis of the Bertillon System. This failure of this system soon led to the development of another physical measurement system, or biometrics—that is, fingerprinting. Sir Francis Galton, a British anthropologist and a cousin of Charles Darwin, is generally credited with developing the scientific method of using fingerprint patterns for identification purposes, although fingerprint pattern recognition actually dates back to the 17th century in Europe.[3] Fingerprinting exists today as a primary means of authenticating an individual's identity. The term has become generic, used to describe unique characteristics about electronic items such as magnetic-stripe cards, personal computers, tablets, and mobile phones that can be mapped.

[1] 1 Kings, Chapter 28, Verse 1, *The Bible*

[2] www.notarypublic.ie/history-of-the-office-of-notary-public/

[3] www.onin.com/fp/fphistory.html

For time-sensitive matters, other ways to provide reliable and speedy authentication have been developed, such as verbal passwords. A weakness of the simple mono-password system was that the password provider had no way to authenticate the password receiver. Such authentication was critical in warfare, when a soldier who approached an unknown person could not readily determine if that person were friend or foe. That failure led to the development of the challenge-and-response method, whereby one party would provide a challenge word or phrase and the other party would respond with a word or phrase. If either party used the incorrect phrase, it was assumed that person was hostile.

Authentication methods can be divided into three groups, also known as *factors*:

- *Something you are* (signature, voice, other biometrics)
- *Something you know* (password, challenge question/answer)
- *Something you have* (payment card, mobile phone)

With the advances in GPS, or global positioning system, technology and its integration into wireless devices, a fourth authentication factor, geolocation—someplace you are—has the potential to be added to the mix.

## Two Faces of Authentication in Payments: The Parties and the Payment Transaction[4]

The authentication of the parties is a core element in any transaction from a variety of perspectives. The authentication of a participant in a transaction defines the party's permission to act as well as the scope of permitted actions. Should a party be admitted who is falsely authenticated, the party who provided that admittance may be liable for the risk to downstream parties. As noted at the beginning of this paper, the authentication of the payment order itself is separate from the authentication of intermediating parties to a payment transaction. Methods such as hashing, seal encoding, or secure electronic signatures can be embedded in a payment order from issuance through every stage of intermediation. These methods can be used to prove that the payment order was properly authorized for a particular amount or date, and that it is payable to a specific beneficiary. This aspect of payment security will be studied in more detail in the next phase of our effort.

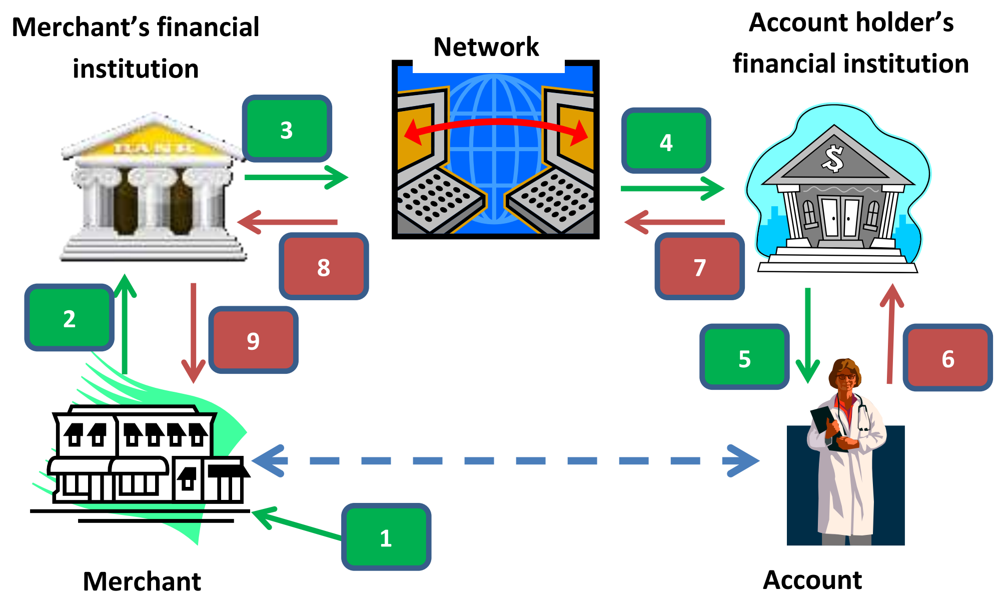
### Checks

In the United States, payment law originated with bills of exchange, then checks were included under the Negotiable Instruments Law. Next came the Uniform Commercial Code (UCC). While the UCC defined various elements of a check that were necessary for it to be considered

[4] Disclaimer: The contents of this section are provided for informational purposes only. They are not intended as and do not constitute legal advice and should not be acted on as such. The materials and links are also not the legal opinions of the Federal Reserve Bank of Atlanta or any of its attorneys, nor are the materials represented as being all-inclusive, correct, complete or up-to-date. No one should rely on any information in this section and we suggest that you should seek the advice of an attorney with respect to any legal issues relative to this matter.

negotiable, the core authentication element was the signature on the check. As the UCC's Articles 3 and 4 were developed, they laid the groundwork for a system in which each party to the transaction warranted the transaction from the previous party. This flow is illustrated in figure 1.

**Figure 1: Check Clearing Process Flow**


Merchant's financial institution
Network
Account holder's financial institution
3
4
8
7
2
9
5
6
1
Merchant
Account

1. Accountholder conveys check to merchant in payment of goods and services. Merchant follows internal procedures to verify identity of presenter.
2. Merchant deposits check into business account at their financial institution (FI).
3. Merchant's FI presents the check to the intermediate clearing network.
4. Clearing network transmits check to account holder's FI.
5. Account holder's FI applies the check against the account holder's account.

Under this scheme, if something were wrong with the check in regard to its authenticity (if it's been altered, counterfeited, forged, or improperly endorsed), there was recourse under the UCC within specified timeframes reversing the original flow all the way back through the process to the bank of first deposit (steps 6–8 in figure 1). Generally, under the customer agreement between the bank and the merchant, the bank would have the right to charge the merchant's account for any items dishonored (step 9). The paying bank, nevertheless, is responsible if it pays a check not properly signed by the account holder and does not execute a timely return or send notice of dishonor (midnight deadline). In the case when a check is presented directly to the account holder's (drawee) bank by the payee, it is the responsibility of the drawee bank to verify the authentication of the item.

Beginning in the 1970s with the bulk filing of checks—checks were no longer sorted in account order on a daily basis—the signature verification process became the exception. Today, the maker's signature on individual checks is rarely authenticated unless the check is for a high-dollar amount or there is some type of security alert on the account. To blunt this exposure on commercial accounts, financial institutions have introduced fee-based services such as "positive pay." Under this service, account holders provide financial institutions with a list of the checks they have created, and the checks presented for payment are compared against that list. If an unlisted check is presented, it normally is returned after the financial institution has performed some level of due diligence to ensure that it is in fact an unauthorized item and not some type of error in the positive pay process.

The risk to the check's payee is the inability to authenticate that the check was made by the account holder, as well as to ensure that there are sufficient collected funds in the account to pay the check. The payee can mitigate these risks by requiring additional identification credentials and by engaging with third parties that provide check guarantee programs. In these programs, the third party reimburses the merchant for any dishonored checks, subject to certain conditions, in exchange for a fee paid for each check accepted by the merchant.

### ACH and Card-Not-Present Credit/Debit Cards

ACH liability for unauthorized transactions is differently aligned, as the originating depository financial institutions (ODFI) is responsible for authenticating that the transaction was authorized by the account holder and, if there is a dispute, is held liable through recourse. Again, through an account holder agreement, the ODFI generally has the right to charge the originating account holder's account for disputed or unauthorized ACH transactions. This recourse is vital to the financial institution since it is the originator who is required to hold proof of the account holder's authorization to initiate the transaction.

It is similar for credit/debit card transactions made online, over the telephone, or through mail order—transactions commonly referred to as "card-not-present" (CNP). This type of transaction is generally "authorized" through the card networks as to the validity of the account number and sufficiency of available funds, but the liability for unauthorized transactions generally shifts back to the merchant. The reason for the shift is there was not a guaranteed authentication directly between the merchant and the cardholder's bank. While Regulation Z for credit cards and Regulation E for debit cards limit the cardholder's liability for unauthorized transactions, it is the card brand's network operating rules that govern the overall chargeback process. There are some exceptions to this scenario—for example, if the merchant uses a secondary authentication method acceptable to the Issuer's network (such as with an online PIN), then the issuer bears the liability for the unauthorized CNP transactions.

### Card-Present Credit/Debit Cards and Wire Transfer

Unlike the check, CNP card, and ACH processes, credit/debit card transactions made in person and wire transfer transactions initiated directly by the authorized account holder are nonrevocable once executed from an authentication standpoint. As with CNP credit/debit cards, the customer's liability is limited by regulation for unauthorized transactions. Generally for card-present transactions, the issuing bank is saddled with the financial loss for the unauthorized transaction. In cases when the cardholder acknowledges that he or she performed the credit card transaction but claims there is an issue with the quality of the goods or services received, the cardholder's dispute falls under the guidance of the card brand's network dispute process. For credit cards, this is controlled by Section 75 of the Consumer Credit Act of 1974. For both credit and debit cards, the cardholder is required to attempt to resolve the dispute with the merchant before filing a dispute with the financial institution.

Wire transfers fall under the scope of Article 4A of the UCC and of the financial institution's customer account agreement. Article 4A was instituted in 1989 to recognize the difference between paper and electronic transactions, since physical signatures and endorsements don't exist in the electronic transaction world. Part 2 of the article deals specifically with the customer originating the payment order and the financial institution that receives the order and that will originate the processing of the payment transaction.

Section 4A-202 (b) allocates the risk of loss from an unauthorized transfer to the sender and not to the sender's bank if the following conditions are met: 1) there is a written agreement between the customer and the financial institution stating that the payment request will be verified using a defined security procedure, 2) the defined "security procedure is a commercially reasonable method of providing security against unauthorized payment orders," and 3) the financial institution accepts the payment request in good faith and follows the defined security procedure.

If the financial institution can prove that it has all these elements in place, the customer must accept the loss of any unauthorized wire transfers. However, if the customer can show that the security procedure was not followed, not commercially reasonable, or breached outside the control of the customer, the financial institution must accept the loss. In many cases, disputes over liability for unauthorized wire transfers end up in litigation due to the large dollar amounts. There have been a wide range of results of such lawsuits since each situation is evaluated individually by the courts.

### Multi-Layered versus Multi-Factor Authentication

These two terms are often incorrectly interchanged but they are two separate security concepts. As its name implies, a multi-layered security application uses two or more elements of the same type of authentication factor laid together. For example, the entry of a password followed by the requirement to correctly answer a knowledge-based question (such as name of first pet, or mother's maiden name) are two types of "things you know."

Multi-factor authentication is the use of two or more separate authentication factor types. An example would be an ATM transaction that requires both a card (something you have) and a personal identification number (something you know) to complete a cash withdrawal. While any authentication scheme that uses more than one layer or factor increases the difficulty of compromising that scheme, it is generally thought that a multi-factor authentication scheme provides a more secure system than a multi-layered system because of the multiple but separate authentication categories required for successful authentication.

### Enrollment Validation

A critical point in any authentication process is when the individual first enrolls as a user or customer. It is then that the individual is required to provide the necessary documentation to prove his or her identity. The number and types of documents needed to authenticate identity vary to a large degree according to the risk level of the program in which the person is enrolling. If it is some type of couponing or loyalty program, documentation requirements are generally minimal, if any. In the case of more sensitive programs, such as opening a bank account, the standard process would require multiple forms of documentation to comply with antiterrorism and anti-money laundering (AML) regulations. To enroll in the Transportation Security Administration's Pre✓™ flyer program, the documentation and overall enrollment process is quite extensive and includes fingerprinting and verification by the FBI that the applicant has not committed a serious crime.

For depository institutions and other covered entities, Section 326 of the U.S. Patriot Act requires the entity opening an account to have in place a customer identification plan (CIP). The purpose of the CIP is to enable the bank to form a reasonable belief that it knows the true identity of each customer within a reasonable period of time after the account is opened. The procedural elements of the CIP are developed individually by each entity based on its own risk model, although the act specifies minimum requirements.

As noted above, the most common form of authenticating a person's identity is through documents, and the most commonly accepted document is a government-issued form of identification that contains a photograph and provides evidence of the customer's nationality or residence. Examples of such identification include driver's licenses, state-issued ID cards, or a passports. Since skilled criminals can alter or forge documents, banks are encouraged to use more than a single document and to examine documents closely to ensure that they are genuine.

In addition to documentary credentials, nondocumentary methods may also be used. A nondocumentary verification can be accomplished by comparing information provided by the customer with information obtained from reliable, third-party sources, such as a consumer reporting agency, another financial institution, or a public database.

### Authentication versus Verification Systems

An *authentication* system is a system that determines if the sample authentication element being presented is a match to the element that was captured when the individual was enrolled. This system is also referred to as 1:1 (one-to-one) matching. These types of programs are the fastest and lowest-cost authentication systems. They are typically what customer authentication systems in banking and payments use. In contrast, a *verification* system has a large database of all the individuals who have been enrolled or whose data has been collected from other sources. This system, also known as a 1:many (one-to-many) system, tries to match the element being presented to the identification of an individual already in the system. For example, law enforcement may try to match a fingerprint taken from a crime scene to its database of fingerprints from individuals with a criminal record.

### Person-to-Person Customer Authentication

#### Visual

As noted at the beginning of this paper, the simplest and fastest method of customer authentication is the visual recognition of the customer. Customers who are frequent visitors to the same banking office often enjoy this recognition and ease in transacting their business without having to show any additional identification. While this method of authentication can be compromised through disguises such as life masks or in the case of identical twins, such scenarios are generally better suited for spy movies than real-life payment authentication. Visual identification represents the fastest and lowest cost method of authentication but lacks documentation should there be a question of authentication after the event.

Source: Wikipedia Commons, public domain

#### Paper Documentation

Personnel who don't have that level of familiarity with customers may resort to asking customers for official documentation, such as a driver's license. In the banking environment, it might be possible for the bank employee to discreetly access the customer account's signature image from the online terminal and visually make a comparison. While slower than visual authentication, the process is generally handled in a timely fashion if the customer has the required documentation. Should documentation be required, the documentation sources, along with key elements of the documentation, are generally noted as evidence that such documentation was produced. Although identification documents can be altered or counterfeited or signatures can be forged, experienced banking personnel can normally spot such attempts so the risk threat is generally considered to be low. The overall efficiency of this system results in minimal operational costs.

#### Verbal Challenge–Response–Countersign

Verbal challenges with password responses and acknowledgements, though rarely used today in public settings, are still used in military and closed social organizations as a way to identify other members. The normal sequence in a military setting is that the guard will speak the predetermined word as a “friend or foe” challenge. The other person then responds with the word or phrase. If the individual fails to provide the proper response, the challenger assumes that he or she is hostile and takes the appropriate action. If the individual provides the proper response, the sentry responds with an acknowledgement word as a countersign, indicating his or her own status as authorized. To be most effective and minimize compromise, the challenge-response-countersign responses should be changed frequently. This authentication method has been adopted by the information technology industry in various electronic ways to authenticate a user’s access to a network.

### Electronic Customer Authentication

As electronic transactions continue to grow, with the expectation for speedy completion and the customer in a remote location, the process of customer authentication has grown more complex. A number of different customer authentication methods have been developed according to the channel being used and the risk level of the transaction attempted. As these different authentication methods emerge, there is a need to balance the effort required to authenticate the customer with its impact on the customer’s overall payment experience. This is commonly referred to as the “level of friction” encountered by the customer. An authentication method that has a high level of friction can present negative consequences: alienating the customer and creating a feeling of dissatisfaction, slowing down throughput resulting in lower efficiency and a reduced service level, or causing the customer to abandon the purchase transaction altogether. In a worst-case scenario, the customer goes to another merchant who is viewed as providing a better experience.

Each of these electronic authentication methods are discussed in more detail below.

Passwords

The most common form of customer authentication is the sign-on password (*something you know*). Password authentication is the least expensive to implement and for the customer to manage, which is primarily why its use has become so common. In its simplest form, the password provides little customer friction, especially when the customer is allowed to select it. The most common exception is when the customer forgets the password and has to contact the financial institution to reset it. This is often done through an automated online or voice response system that uses challenge questions to authenticate the customer before the customer selects a new password. The necessity of supporting password resets can result in costly staffing efforts.

Unfortunately, since it is the simplest form of electronic authentication, a password is usually the weakest model because, for many users, passwords can be guessed easily or illicitly obtained. A 2013 study by UK-based password management application vendor SplashData[5] found that "123456" was the most common password, followed by "password." A similar study of 1,800 adults found that approximately 25 percent used passwords that were easy to guess, such as birthdays or names. Moreover, more than half (55 percent) admitted that they used the same password for access to multiple websites.[6]

How do you reconcile such behavior with the consistent research findings that consumers view security and privacy as their primary concerns regarding online usage? Unfortunately, the reality is that while people aspire to protect their security and identity, when faced with a choice that requires additional effort or friction, they most often choose the easier, less secure way. This behavior can be seen in many other forms of human behavior—when someone says he or she wants better health but continues to smoke, or when someone wants to lose weight but continues to eat junk food, or when an individual wants to become more financially stable but doesn't develop a financial plan with a savings component. Continued education about password security is essential from financial institutions and any other companies that require a password to access their websites or applications.

Security experts generally recommend the following password practices to provide more secure password management.

- Select a strong password that incorporates lower- and uppercase letters, numbers, and special characters and that has an absolute minimum of eight characters.
- Swap characters or numbers for letters, such as $ for the letter *S* or 1 for the letter *L*.

[5] www.telegraph.co.uk/technology/news/10587694/Worst-password-of-2013-was-123456-according-to-new-research.html

[6] Ofcom, UK Adults Taking Online Password Security Risks, April 23, 2013

- Avoid using the same password for multiple sites by taking a base word and then appending it with some part of the website name. For example, using the base word **$anter14**, the password would be **Tr@il$anter14** for a hiking trails website. Deliberately misspelling a base word also makes it more difficult to crack since password hackers often use a dictionary tool in automated password attacks.
- Change your passwords frequently, preferably quarterly but at least annually, on any website involving sensitive financial or personal information. Change it annually on nonsensitive websites. You can add the first three letters of the current month to the appended password. In the example above, assuming the month of April, the password could be **AprTr@il$anter14** or **Tr@il$anter14Apr**.
- Don't write your password down or give it to others. If you feel you must make a written note, write only a hint or a description of the password structure, and do it in a shorthand that only you can decipher.

While enforcing a requirement for strong passwords or password changes is often used to increase the difficulty of a criminal compromising an individual's account authentication credentials, such a requirement has the potential negative impact of not allowing a legitimate user to access an application when he or she forgets the password. A recent study by the Ponemon Institute[7] revealed that 46 percent of U.S. respondents couldn't complete a purchase or account transaction because of authentication problems, which caused them to view the company negatively.

Unless strong password practices are mandated—as is often the case in corporate environments, where such policies can easily be enforced—most industry observers believe that passwords represent a minimal level of security and can easily be compromised. Although they are easy to implement in applications, as noted earlier, there can be substantial support costs related to their management and reissuance to customers. More and more companies are looking to implement additional authentication methods for moderate- to high-value transactions to minimize risk.

### Knowledge-Based Authentication (KBA)

Sometimes referred to as "challenge questions," KBA is generally used as an additional authentication layer (*something you know*) when an ID or password is not sufficient or when a user has forgotten the password and has to have it retrieved or reset. There are two classifications of KBA: static and dynamic. A static KBA process requires the user, during the account setup sequence, to select from a predefined list of questions and to provide the answers (table 1). Some programs allow customers to select their own questions.

[7] Moving Beyond Passwords: Consumer Attitudes on Online Authentication, Ponemon Institute, LLC, April 2013

**Table 1: Sample Static Knowledge-Based Authentication Questions**

| | |
|---|---|
| 1. | What is the name of the street on which you grew up? |
| 2. | What is the name of your favorite book? |
| 3. | What is the last name of the best man at your wedding? |
| 4. | What airline do you prefer to fly? |
| 5. | What was your first pet’s name? |
| 6. | What is the name of your favorite sports team? |
| 7. | What is your favorite color? |

The program stores the selected questions and answers and uses them when necessary. The difficulty level in a fraudster compromising a static KBA process depends on the difficulty of the questions. Given the high amount of personal data that is available through government records and social media, questions such as mother’s maiden name, pet’s name, city of birth, and so on provide minimal protection. Any criminal seeking to compromise the account credentials can often find such information easily and can then reset the account password and gain access to the account. For this reason, more static KBA processes are using questions whose answers are not so readily available through other data sources—for example, favorite childhood cartoon character or favorite high school subject. Similar to the implementation of strong password practices, there is always the challenge of balancing the uniqueness of the question with the legitimate user’s ability to remember the answer initially provided.

To address these weaknesses, some companies use a dynamic KBA, or “out-of-wallet” question-and-answer process. In this case, users must answer questions not known beforehand but ones to which the genuine user should be able to correctly respond. This information is generally obtained from the individual’s credit report or transaction history file with the company. Sample questions might include choosing from a list an address where you never resided, the approximate range of your current monthly car or house payment amount, or the date of your last bank account deposit. While a dynamic KBA is not foolproof, as the criminal might have obtained the victim’s credit report or account records to provide the answers, the method is considered to provide a higher level of security than a static KBA process.

Static KBAs are fairly easy to implement and operate but, again, they require support in the event the user cannot get through this authentication filter. Dynamic KBAs provide a higher level of security, but they are more expensive because generating them requires live feeds to account or third-party databases. They also require a support system in case a customer fails the authentication.

### Site Keys

A number of websites, especially those supporting financial services and transactions, have recently adopted site keys. The purpose of the site key is to provide an electronic variation of the challenge-response-countersign authentication method discussed earlier. In this case, the user enters his or her user ID and before, the user enters the password, the website returns a page that displays a graphic image that the user has preselected. Identifying this image demonstrates to the customer that he or she is interacting with the legitimate website, not a counterfeit. Once the user has seen the site key, the user is prompted to enter the password to complete the authentication sequence. The use of site keys has gained more popularity in recent years due to the increased number of spoofed websites where the victim is tricked into making an inappropriate yet security-relevant decision, such as revealing online banking sign-on credentials or payment card numbers. Site keys can enhance existing logon systems and create little user friction other than asking them to verify the image as correct before continuing to log on.

Security Tokens

These tokens are referred to by a variety of names: hardware tokens, authentication tokens, USB tokens, cryptographic tokens, one-time-password (OTP) tokens, and more. Security tokens are used as part of a multi-factor authentication environment. The physical token provides the *something you have* security factor with *something you know* in the form of a password or ID. The use of a security token that incorporates one-time passwords prevents replay attacks if an intruder has monitored previous sessions and obtained the log-in credentials since the password changes for each subsequent log-in the previous data will not work.

Source: Cryptocard - Used with permission

The tokens can generally be classified as either disconnected or connected tokens. With a connected token, the user inserts the token into some port on the device and attempts to log in to the network. The user must then enter the token’s password. The token checks the entered password with the password that was encrypted and stored in the token at enrollment. If there is a match, the token passes the appropriate credentials to the network and gives the user access.

A disconnected token can be in many different form factors, including key fobs and cards. In general, the token device has been time synchronized with the host computer to generate a distinct code at a specified interval (usually every minute or less). The user must enter that code, along with regular sign-on credentials, to get access to the network.

If a token is lost or stolen, the multi-factor aspect of its operation prevents any major risk issue since it is presumed the thief does not have the token’s password. Most token management systems disable a token after a small number of incorrect attempts to prevent a brute force password attack or to keep the thief from guessing the password by trying frequently used password structures.

The tokens are durable and cannot be reverse engineered, so they are physically secure. USB security tokens have the advantage of not requiring a battery since they are powered by the device they are plugged into, while a disconnected token does require a battery that generally has a life of approximately 10 years. While security tokens are relatively inexpensive, they do require a token management system with the appropriate level of controls and administration.

Some banks outside the United States are piloting disconnected tokens to handle online banking validation or combat mobile commerce fraud when there is no merchant terminal or card interaction to validate the presence or authenticity of a payment card. As with other authentication methods that this paper discusses, the "password" tokens require additional steps for the customer before access is granted and require the customer to maintain possession of this separate device. Although they provide a high level of security in a two-factor configuration, the cost and management of the tokens have discouraged many banks and businesses from pursuing this method.

Online PIN/3-D Secure

Payment studies have consistently shown that the use of a PIN with a debit card transaction results in a substantially lower rate of fraudulent transactions than do signature debit card transactions. The 2013 triennial payments study conducted by the Federal Reserve found that signature debit transaction fraud was almost four times higher than PIN debit fraud.[8] With electronic commerce and its environment of CNP, the payments industry has been searching for ways to improve authentication and reduce fraud. As the United States migrates to EMV chip cards, there is the expectation, based on results of other countries that have migrated to EMV, that counterfeit card fraud will largely shift to CNP transactions. Primary solutions are generically referred to as online PIN and 3-D secure.

- Randomized online PIN: A solution developed by one vendor, Acculynk, has the customer enter the debit card PIN on the merchant's shopping checkout screen, which randomizes the placement of the numeric keys to defeat keylogging and other malware programs. The merchant controls whether the PIN entry is required based on their risk management program.
- 3-D secure: The name comes from the goal of securing electronic commerce transactions among the three stakeholder domains: cardholder, merchant, and the cardholder's financial institution. MasterCard operates the product under the name SecureCode; Visa, under Verified by Visa; and American Express, under SafeKey. When first introduced in 2010, the product met with poor acceptance by merchants and consumers for a variety of reasons outside of pricing. The method directed the customer to another website for all transactions, which ran counter to general internet security warnings to consumers of

[8] https://www.frbservices.org/files/communications/pdf/research/2013_payments_study_summary.pdf, page 35

being leery of pop-up windows or web page redirects. Additionally, all online transactions for that merchant had to be handled through the service. Since the service was restructured in 2014, there has been an expectation for greater merchant acceptance. The feature is more seamlessly integrated into the merchant's checkout process. The merchant decides whether or not to require the feature's use on a particular transaction based on the merchant's own risk management program considering the customer and purchase transaction parameters.

**Biometrics**

Biometric authentication uses one or more of a person's physical attributes to validate the person's identity. The controlled and validated enrollment of the individual and that individual's biometrics is absolutely essential. This enrollment is normally conducted in a secure, controlled manner to guard against introducing an imposter into the program.

Positive versus Negative Identification

Biometric identification systems can be divided into two types: *positive identification* and *negative identification*. The positive identification system verifies that the biometrics are from an individual known to the system, preventing multiple users of a single identity. An example of this positive identification system would be a biometric fingerprint system used to control access to a laboratory—an individual requesting access swipes or inserts a card with a fingerprint template, and then places his or her finger on the reader. The system then retrieves the fingerprint template created at enrollment and compares it to the fingerprint template generated from the "live" fingerprint reader. If they match within specified tolerances, the door unlocks, granting the individual access. Such a design uses multi-factor authentication by combining *what you have* (card) with *what you are* (fingerprint). To further increase the security level, such a system could add a step—for example, after swiping his or her card, the individual could be required to enter a personal identification number (*something you know*).

The fingerprint template captured at enrollment may be stored in a central database or may reside as a mathematical value on the card. In the central database configuration, the reader must have a connection to the database to match the "live" fingerprint template with the one in the database. But if the enrolled fingerprint template value is stored on the card, there is no need for online access. In this case, there would have to be data storage capability within the reader device to record the entry attempts. Financial institutions use positive identification systems for authenticating users conducting banking transactions.

A negative identification system is intended to prevent an individual from creating multiple identities by ensuring that the person's biometrics don't match an identity already enrolled in the system. A voter registration program using biometrics is an example of a negative identification system. In such a program, the individual provides the biometrics, like a fingerprint.

The system reads the fingerprint and generates a template whose value is matched against all other identities already registered in the system. If no match is found, the enrollment proceeds. If a match is found, the individual is already registered and so the enrollment is canceled. A positive identification system does not require the use of biometrics since other forms of identification can be used to establish the person's identity, while the negative identification does requires submittal of the biometrics because no alternative methods exist for verifying a claim of no known identity.

Biometric System Elements

In addition to the classification discussed above, there are other elements that can be used to classify and distinguish biometric systems. These elements include:

- **Overt versus covert**: With an overt system, users are fully aware that their biometric data are being collected and used. Conversely, with a covert system, the user is unaware their biometric data is being collected.
- **Public versus private**: Private systems include only a limited group of affiliated individuals (that is, employees) while public systems incorporate customers or other members of the general public.
- **Template versus image:** A biometric system providing greater user privacy is one that collects the biometric data and then processes it through a mathematical algorithm to produce a template or mathematical value. If the image of the human sample—such as a fingerprint—is retained, it would be possible to reproduce that image and subsequently associate it with a specific individual.
- **Open versus closed:** A closed system is one in which the biometric data will not be shared with any other party. A facial recognition system used only in the employee's building to control physical access is an example of a closed system. On the other hand, if the data are shared with other parties, it is considered an open system. An example would be a fingerprint captured as part of an application for a governmental background check might be shared with other governmental or law enforcement agencies.
- **Optional versus mandatory:** If the user is required to participate in a biometric authentication program and refusal to do so results in some sort of punitive action, it is considered mandatory. Employees of a company with restricted-access facilities will be required to provide some biometric sample to be able to work in that facility. Optional programs allow individuals 0 to decline participation although normally some other form of identification will be required.
- **Standard versus noncontrolled environment**: A standard environment is generally one that is indoors, where such environment factors as temperature, humidity, and lighting can be controlled to optimize the performance of the biometric data capture device. An

exterior or variable public environment is subjected to a much wider range of those environmental elements and may affect accuracy and device hardening costs.

- **Fixed versus indefinite duration**: This element refers to whether the biometric data captured at enrollment will be deleted or destroyed after a certain amount of time or in response to an event—for example, at termination of employment—or whether it will be retained for an indefinite period.
- **Frequent versus infrequent usage:** This characteristic is based on the frequency with which the user will be interacting with the system. Biometric systems that have infrequent usage may require a simpler user interface since learning how to use the system will not be reinforced with repetitive usage in a short period of time.
- **Supervised versus nonsupervised**: While the enrollment process is almost always supervised with some level of human involvement and oversight, the actual use of the system may not require such involvement (nonsupervised).
- **User versus institutional data ownership:** A system may be operated whereby the user maintains control and ownership of the biometric data used in the system—for example, the user has ownership of the access card containing his or her biometric template, with no central site storage—or the institution retains ownership. Very few systems are under user ownership, although legal rights governing how the data can be used can be provided through a separate agreement.

### Biometric System Accuracy

It is important to note a key difference between biometrics and other electronic authentication methods such as passwords and KBA. With the last two, if there is not a 100 percent match between the authentication data on file and the data entered by the user attempting to gain access, the request is automatically rejected. While it may be the legitimate user trying to gain access—say the user forgot the password—the system rules prevent access until the user's identity can be authenticated through some other means.

On the other hand, the nature of biometrics is such that rarely is there a 100 percent match between the stored template value and the live template value because of differences in lighting conditions, for example,  or angles where the biometric measurement is made, or differences between readers. The manager of each application has to determine the "score" or accuracy level that is acceptable for both false-positives (whereby a party who incorrectly matched is authorized) and false-negatives (whereby the authentic party is denied access). Naturally, the false-positive response poses the greater threat; the false-negatives generally just involve some level of inconvenience until the individual can be authenticated and provided access.

### Biometric System Characteristics

So how do you measure which biometric system is the best one for your application? The ideal biometric system can be determined in the measurement of more than six key characteristics, listed in table 2.

**Table 2: Biometric Method Characteristics**

| Characteristic | Description | Quantitative Measurement |
|---|---|---|
| Robustness | Lack of change over time | Submitted sample does not match the enrolled template (false non-match) |
| Distinctiveness | Large variation over the population | Submitted sample matches the enrolled template of another individual (false match) |
| Accessibility | Ease in taking measurements | Number of individuals who can be enrolled in a given time period (throughput) |
| Availability | Entire population should be measurable | Number of individuals who cannot be enrolled due to an inability to supply a readable measurement (failure to capture/enroll) |
| Acceptability | Population does not object to having the measurements taken | Attitudinal research |
| Financial | Cost of implementing and operating | Acquisition, implementation, and operating costs |

One other distinction among types of biometric measurements is whether they are physical or behavioral. Keystroke dynamics, gait analysis, gesture dynamics, and handwriting are all classified as behavioral biometrics. With the exception of handwriting, the others are relatively new measurement systems and have not been proven to be as accurate as physical biometric systems.

### Biometric Methods

The primary biometric methods covered in this working paper are fingerprint, hand/finger/palm geometry, facial recognition, iris recognition, retina scan, voice, and signature recognition. We also discuss DNA and other behavioral biometric methods. These technologies are discussed in more detail below.

Source: FBI – Public Domain

Fingerprints – Fingerprints are truly unique among individuals, including identical twins, and remain constant throughout life. For this reason they serve as a nonrepudiated form of identification and represent the most widespread use of biometrics, especially in criminal justice applications. The FBI claims to have the world's largest database of fingerprints in its Next Generation Identification (NGI) system launched in September 2014,[9] with more than one hundred million records of finger and palm prints. NGI replaced the FBI's Integrated Automated Fingerprint ID System (IAFIS) that was fully deployed in 1999. The system has also begun adding iris recognition and mug shots to its database.

As with other biometric methods, the enrollment process is critical for fingerprint readers encased in devices such as laptops and mobile phones. The process is more of a challenge for these devices as the application provider must often deal with a customer who is remote, so the provider has to employ other authentication methods to first validate the identity of the person and then verify authority to access the designated account.

The mildly invasive process involves the optical or electrical capacitance capture of the pattern of ridges and valleys (furrows) on the fingertips as well as points where a ridge divides or ends (minutiae points) by placing fingers on the reader. After capture, a template of the fingerprint is created using mathematical formulas. While an optical image of the fingerprint may be captured, most systems discard the original image for security and privacy reasons and maintain only the digitized fingerprint template, which is further secured through cryptography. It is critical to initially achieve a high-quality capture of the fingerprints to provide more accurate comparisons on subsequent authentication efforts. Studies have shown that obtaining high-quality fingerprints from certain sections of the population such as the elderly and manual laborers can be difficult due to poor fingerprint characteristics.

To address that problem, several vendors[10] have recently introduced or announced plans to introduce an ultrasound fingerprint reader that creates a 3-D image and then generates a template of that image. One vendor claims a false-positive rate of 1:10 million. Currently available only on external device readers, the vendors plan to integrate it into various mobile phone models in 2015. The 3-D image is reputed to produce a more detailed template as it penetrates the outer layer of the skin, which is what is captured in a two-dimensional capacitive reader on some current mobile phones.

While technology advancements continue to provide higher-resolution and higher-quality readers at lower costs, a high-performance commercial system is moderately expensive to acquire and maintain. While rugged, portable readers have been produced, the ideal setup is in a clean, climate-controlled environment. It should be noted that while the Apple iPhone 5s and Samsung Galaxy S5 smartphones introduced fingerprint readers to their users in 2013–14 as an alternative to a password to unlock the handset, the resolution of the reader is not comparable to a commercial system's in terms of the reliability or accuracy. Apple has stated that the odds

[9] http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system

[10] http://www.cnet.com/news/qualcomm-snapdragon-sense-id-3d-fingerprint-scanner-hands-on/

of someone else’s fingerprint receiving a “match” (false positive) is 1:50,000.[11] Since the phone allows only five unsuccessful attempts before requiring entry of a four-digit passcode (which has a 1:10,000 probability of being guessed), this level of resolution is probably sufficient for simply unlocking the phone. However, with the introduction of the iPhone 6 and its Apple Pay mobile payment capability, whereby the phone uses the fingerprint reader to verify the phone owner is performing the transaction (with the passcode as a backup), care must be taken to understand the risk level of granting the wrong person access to the application on the phone. This will become more critical as third-party developers are allowed to create applications that use the fingerprint reader as the sole authentication method.

Fingerprint readers on ATMs have failed to gain any traction in the United States but have been successfully implemented in Brazil, where approximately one-third of the ATMs in the country have been retrofitted with fingerprint or palm print readers. Depending on the bank, a customer may not even have to insert a card; the fingerprint is used to access the customer’s authorized accounts. Other banks use the fingerprint template verification in place of the PIN, but the customer still inserts the payment card.

Hand/Finger/Palm Geometry – After fingerprinting and handwriting, hand geometry represents the longest-operating biometric system; the first commercial application was introduced in 1981. The 1996 Olympic Games held in Atlanta, Georgia used a hand geometry application to provide access control to the Olympic Village by the athletes and other authorized personnel. Hand/palm geometry applications use features such as finger length, finger width, finger thickness, finger area, and palm width to identify a person. The system is considered only mildly invasive. Since the palm represents a larger area than a finger, it offers the ability to capture more distinctive features than fingerprints.

Source: FBI – Public Domain

Since finger geometry is not unique, this biometric must be used with another form of authentication in large user populations to properly authenticate an individual. For this reason, developers began to incorporate palm prints into the overall hand geometry system since palms have many of the same pattern determination elements that fingerprints provide.

While procedures may vary depending on the specific application, in the enrollment process, individuals are instructed to place their hands on the reader several times so multiple images can be captured and then averaged to form the enrollment template. Usually the enrollment process can be completed in less than 10 seconds.

To authenticate users, the users place their hand on the reader. The image is captured and converted to a template, which is compared against the template developed during the enrollment process. The authentication decision can be made within a couple of seconds.

Some major advantages of hand geometry systems are that they work well in harsh or dirty environments such as industrial sites, have the ability to capture both finger and palm prints in one scan, and the hand template generates a modest-sized digital data set. Since the process

[11] www.support.apple.com/kb/ht5949

does require more expensive, larger reader devices, the system is generally best suited for access control. However, costs have been coming down and a number of banks in India and Brazil have incorporated the readers into their ATMs. . Some banking institutions in the United States are piloting hand/palm geometry readers in their safe deposit box access applications. Like other biometric systems, the enrollment process is critical to ensure the individual being enrolled is authenticated and authorized.

Vein Recognition – An emerging biometric first developed in 2005 is that of obtaining an image of the vein patterns in the finger or back of the hand, which are unique to every individual. The image is captured when the individual places the finger(s) or back of the hand above a device containing a near infrared light and a monochrome charge-coupled device (CCD) camera. The hemoglobin in the veins absorbs the near infrared light and creates a pattern of lines that does not change as the individual ages. The camera captures this image, which is then mathematically converted into a template. These patterns are almost impossible to counterfeit since they are located below the skin's surface and are present only people who are living. As with fingerprint and hand/palm geometry systems, this system is considered to be minimally invasive since it doesn't require the placement of the hand on the device itself.

While this type of biometric system represents only about 5 percent of the overall biometric solution market, it is one of the fastest growing. More than 85 percent of the ATMs in Japan use vein recognition as the primary means for authenticating the cardholder.

Facial Recognition – Facial recognition is one of the most flexible and discreet authentication methods in operation as it is often used when the person is unaware of being scanned. It represents a technology solution to humanity's first authentication system. Facial recognition systems work by systematically analyzing some of the 80 specific features that are common to the face, known as nodal points—for example, the distance between the eyes, width of the nose, position of cheekbones, depth of the eye sockets, jaw line, and chin. These numerical quantities are then converted into a binary code template, known as a faceprint, which uniquely identifies each person.

Facial recognition applications can be divided in two categories: random scene and controlled scene. In a controlled-scene environment, the individual's facial image is captured in an environment where there is controlled lighting and minimal visual complexity in the background, and the individual may have a marked location on which to stand and face the camera for the image to be captured. These applications are clearly overt and generally located in company or government facilities for access control purposes. Random scene applications are used in public locations such as airports, mass transportation centers, and other gathering locations to aid in the spotting of criminals or other individuals of interest. As expected, a random scene application faces a number of challenges due to varied lighting, viewing angles, background complexity, and distance of the subject to the camera.

The technology was first used in the 1960s in a highly manual process whereby the operator had to locate and designate key facial features such as the eyes and nose before the system began to take automated measurements. Beginning in 2000–01, the facial recognition system received a lot of attention, with the hope that it would provide a means of identifying terrorists or criminals in public gathering locations. The city of Virginia Beach, Virginia, placed cameras along their beach boardwalk hoping to identify criminals and runaway children. For the 2001 Super Bowl, Tampa, Florida, used the system to try to identify known criminals around the Super Bowl venue. After the Super Bowl, the cameras were redeployed in the Ybor City entertainment district. Following the 9/11 terrorist attacks, the technology gained even greater attention. Boston's Logan Airport, the airport used by a number of the 9/11 terrorists to board their airplanes, also tested the system.

During this period, facial recognition technology used systems that attempted to match a two-dimensional (2-D) face with a 2-D image in the database. The systems had poor overall performance as the facial image capture was performed in a random scene environment so the facial image had different lighting, distances, and angles to the camera. In the case of Boston's three-month pilot program, the system recognized the volunteer targets listed in the database as terrorists only 61 percent of the time,[12] so it was scrubbed. The Tampa police department discontinued the Ybor City system in August 2003, citing the ineffectiveness of the system. The Virginia Beach facial recognition system was discontinued in 2005. Police Chief Jake Jacocks Jr. said, "Technologically, it is not advanced enough to be effectively used as we had attempted. It is very effective in casinos, airports, correctional institutions, and other controlled environments."[13]

The introduction of 3-D camera technology and other technological advancements since 2006 has improved the performance of the system, although it does not function at the speed or accuracy often depicted on criminal shows on television. As with all biometric systems, the speed of validating a user in a 1:1 setting is much faster than in a one-to-many setting, where a large database population has to be checked to determine if there is a match.

The authentication of an individual using facial recognition is a six-step process.

1. Detection—the subject's live image is captured and separated from the crowd.
2. Alignment—the position, size, and camera angle of the face are determined.
3. Measurement—the various facial nodal points are measured.
4. Representation—a template is created through mathematical algorithm.
5. Matching—the template is checked against other templates in the database.
6. Verification/Identification—a decision is made as to whether there is a match to another template already in the database.

The newer facial recognition systems have been deployed at casinos, border crossings, and mass transportation locations to help spot known criminals or terrorists. Accuracy results can be impacted by people attempting to disguise their faces with hats, glasses, different hairstyles, and facial hair, all of which make the measurement process more difficult and can lead to a lower confidence level of the resulting facial templates. The unique advantage of a facial recognition system is its ability to be used in a large group setting. Another potential advantage, although it

[12] 'Face testing' at Logan is found lacking. *Boston Globe*, July 17, 2002

[13] http://hamptonroads.com/node/317161

may lead to lower authentication matches, is the ability to create the template database from existing 2-D photographs rather than through a 3-D camera system.

Since most mobile phones are equipped with cameras, there have been some initial efforts to use facial recognition as an additional authentication factor for banking application sign-on, and this biometric method is expected to grow. In January 2015, the financial services company USAA[14] announced that it was supporting facial recognition (along with voice recognition) as an optional online banking sign-on method for its members.

Facial Thermogram – A thermogram is a display that shows the amount of infrared energy that is emitted, transmitted, and reflected from an object. The varying levels are converted into a temperature and displayed as an image. Thermograms have been used in the construction industry for some time to locate areas in a structure where there are dramatic temperature variations, indicating improper insulation or poor quality construction leaving gaps in heated spaces. Fire departments use thermographic cameras to help detect abnormal temperatures inside closed walls that would indicate flames or embers from a fire that is not directly visible. Due to its noninvasive nature, the technology is also being tested in medical research to determine if it could provide an early indication of certain diseases.

In the mid-1990s, scientist Francine Prokoski proved that facial thermograms are unique to individuals. The different heat patterns in the human face are created by the blood vessels branching throughout the facial skin. The technology uses a high-resolution infrared camera to capture the thermograph. While significantly more expensive than a digital camera used in facial recognition systems, the results can be more accurate in places where there are varying lighting and other environmental factors. Like regular facial recognition, people can disguise or alter some of the reading with glasses and facial hair, but these efforts can often be mitigated by "removing" the obstructions with mathematical formulas. Due to the type of camera required and its related expense, facial thermograms are not suitable for consumer authentication applications at this time.

Iris Recognition – An image of the iris (the visible ring around the eye's pupil) also provides unique biometric data elements that are very difficult to duplicate and that do not change after the age of 10 months. A number of advances have been made in iris recognition systems over the last decade, and it is becoming a widely deployed system, especially by the military and prison systems. While the initial iris capture can be difficult to make for children or the infirm, devices have been improved to lessen the capture time as well as measure both eyes at the same time, and they require the subject to blink to prove they are alive.

While the term iris "scan" is sometimes used, this is a misnomer since there is no scanning of the eye. The system is considered noninvasive since it does not involve any contact with the measurement device that is taking a video of the iris. From the video captured by an integrated light source in the near infrared wavelength band , a series of frames are obtained to define the up-to-240 measurement points from which the calculations will be made to create the template.

[14] https://communities.usaa.com/t5/Press-Releases/USAA-Rolling-Out-Biometric-Logon-to-Accounts-in-Q1/ba-p/55785

Source: FBI – Public Domain

The matching process is considered one of the fastest of any of the biometric systems because of its small byte size (512) of the template. Furthermore, it can provide a decision in less than two seconds. The subject is generally required to be within 10 inches of the video camera. Eyeglasses do not affect the quality of the read. Studies have shown the system has a false acceptance rate of 1: 1.2 million.[15] While used today primarily in military and private companies for access control, the technology is expanding into health care and national identification programs in other parts of the world. The challenge in using mobile phones to perform the iris recognition capture is that none of the phones on the market today have the required near infrared light source, although vendors indicated they expect mobile manufacturers to start incorporating them in the near future.

Retinal Scan – Like fingerprints, there is no known way to replicate a retina, as the pattern of the blood vessels at the back of the eye is unique and constant for a lifetime. The concept of using the retina as a means of identification was first described in a *Time Magazine* article in 1935,[16] but the first commercial scanner was not developed until 1975 and systems did not begin operating until the 1980s. Despite being frequently shown in high-tech movies and TV shows, retinal scan systems have not achieved widespread use because of system costs, high false-reject rates and, user vision health concerns. The method has found usage as an access-control application for highly secure military and government facilities, where enrollment is mandated. The system is considered moderately invasive since the enrollment and access read require an individual to place the eye on an eyepiece that projects a low-power infrared beam of light to the retina located at the back of the eyeball. The light beam does a complete 360-degree scan of the retina and captures up to 400 measurements. It requires about 10–15 seconds of careful concentration to achieve the necessary high-quality scan. It is not uncommon for the person enrolling or seeking verification to have to undergo multiple efforts to capture an acceptable image.

After a successful capture, the image is reduced to about 200 reference points and the resulting template is 96 bytes—one of the smallest template memory footprints among all the biometric systems. Successful retinal scans are regarded as highly accurate, although the quality of a read can be affected by someone having cataracts, glaucoma, or severe astigmatism. While delivering highly accurate authentication rates, the technology is not suitable at this time for payment applications because of its cost and consumer health concerns about its high level of invasiveness.

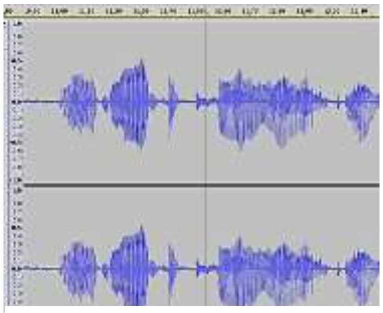
[15] http://irisid.com/howitcompares

[16] http://content.time.com/time/magazine/article/0,9171,755453,00.html

Source: FBI – Public Domain

Signature Recognition – A person’s signature is another example of biometric data easy to gather and not physically intrusive. Signature recognition is essentially a subset of handwriting analysis and considered a behavioral biometric in that signatures can be modified by the user over time. To enroll a signature, after a person’s identity has been verified through the use of other authentication methods, the person is asked to execute the signature on a special signature pad or tablet a number (5–6) of times. The electronics in the device measure the amounts of pressure, acceleration, speed, rhythm, and movements of the device used to create a signature template. These measurements are converted into a template and stored to verify future signatures. Some signature biometric systems can continually update the template since it is normal for a person’s signature to have slight variations each time it is executed.

Signature recognition systems have not been widely deployed due to a number of disadvantages, the most significant being the variation that occurs in a person’s signature—especially when compared to the physical biometrics that are unique and fixed. Signature recognition systems require specialized, moderately expensive devices to capture the signature, create the template, and transmit to the database. These devices are generally not integrated into the devices used by the consumer, although there have been some signature recognition applications developed for use on touchscreen laptops, tables, and smartphones.



Source: FBI – Public Domain

Voice Recognition: Like facial recognition, a voice recognition system provides a way to overtly or covertly authenticate the identity of an individual. While sometimes the terms are incorrectly used interchangeably, a speech recognition system is one that recognizes spoken words and converts them into digital data for executing programmed instructions. Voice response units (VRUs) were the most common form of speech recognition hardware for consumers; the customer speaks a number or a keyword instead of pressing the number on the phone’s keypad. Apple’s Siri application is another form of speech recognition software, and voice-to-text applications are now common on laptops and smartphones. The technology for speech recognition systems has improved greatly over the last several years and reached acceptable levels for information applications.

Voice recognition systems operate like other biometric systems. The individual’s identity is enrolled and authenticated when the person speaks scripted phrases, numbers, or free text. The resulting audio file is used to create a voice template, or “voiceprint.” The template is then digitized and stored in a database. When the individual tries to access the system the next time, the voiceprint of the current connection is compared to the template on file. There remain concerns about the accuracy rate of this biometric outside of controlled audio environments since there are a number of ways to disguise or alter one’s real voice with software or hardware technology. The accuracy can also be affected by the quality of the connection—background noise, a poor telephone carrier connection, or a low-quality microphone can alter the voice. The threat of a criminal using a recorded voice of the actual individual can easily be thwarted by requiring the individual to speak a random phrase.

Due to the accuracy limitations, voice recognition systems are often coupled with other authentication methods. In the case of mobile phones, this could be the phone's device information as well as geolocation data. In the case of land lines, subscriber information can be used to determine if the number being used could reasonably be tied to the legitimate account holder. As mentioned earlier, USAA announced in January 2015 that it was supporting voice recognition as a way for members to access their mobile banking application. Call centers at banks and other financial services companies have used voice recognition systems, usually covertly, to help authenticate customers.

DNA – DNA, or deoxyribonucleic acid, is the hereditary material of life. Nearly every cell in a person's body has the same DNA. Every human's DNA is unique, except for identical twins. Advances in DNA research have made it the definitive element for authenticating an individual's identity and heritage. Since DNA is present in all cells of the human body, the ability to match a sample to a verified enrollment is intrinsically digital and foolproof. Obtaining a sample can be as minimally invasive as a mouth swab.

One of the primary drawbacks to DNA matching for online authentication is the normal timeframe of 60–72 hours to obtain high-confidence matching. Primarily driven by the FBI's efforts, a rapid-DNA initiative has been under way to develop equipment to produce DNA results with high levels of confidence and provide initial results within 90–120 minutes. While this timeframe is still not sufficient for real-time payment environments, it works well for law enforcement purposes.

**Soft Biometrics:** Various physical feature elements that are not by themselves distinctive enough nor do they have the permanence to distinguish an individual are known as soft biometrics. Examples include gender, age, eye and hair color, tattoos, and other distinguishing features such as scars, birthmarks, and moles. These elements can be used as supplemental data to increase the confidence level of the accuracy of the overall authentication decision. Another benefit for the use of soft biometrics has been in a one-to-many comparison effort of a large database, where the additional elements can be used to reduce the scope of the overall database.

**Other Behavioral Biometrics:** In addition to handwriting and signature recognition, a new field of biometrics deals with the consistent behavior of certain muscular and skill-based functions performed by an individual, such as typing (keystroke), walking, and gesture patterns. The underlying theory is that a person's repetitive actions are predictable. Most security experts agree that behavioral biometrics, with the exception of handwriting, are not as reliable as physical biometrics. The walking or gait biometric method is not suitable for banking or payment applications by its very nature of requiring time and space to acquire a sufficient amount of data to form a template. However, typing and gesture biometric authentication applications have been piloted in the banking environment.

In the typing biometric, the individual's pattern of keystrokes is measured in two ways: interkey (flight) and hold (dwell) times. The interkey time refers to the latency period between keystrokes. The hold time represents the amount of time the key is depressed. The biometric calculations can be done so that the overall typing speed of the individual is not relevant. Not sufficiently unique to stand on its own, a typing biometric can be used as an additional authentication factor for a person using an access device with a keyboard. One of the advantages of this biometric is the ability to constantly analyze the patterns created by the user and update the template value. One of the disadvantages is the difficulty of distinguishing between the multiple devices that an individual can use to log in to an account. For example, in this day and age, it is entirely feasible that a user could access a bank account with a desktop computer, laptop, tablet, or mobile phone—which, because of different keyboard ergonomics, would likely result in very different templates for each of those devices.

Source: EPA – Public Domain

Gesture biometrics applications can be used by an individual with a smartphone that has an embedded accelerometer or a computer with a mouse. In the latter case, the individual is instructed to perform a series of repetitive motions with the mouse. The application measures the angle, speed, direction, and length of the mouse movements. In a test program at the multiple campus locations in the University of Texas system, 99 percent of the participants were able to enroll successfully and be validated; they felt it was an overall positive experience.17 With the smartphone, the user performs one of more specific gestures while holding the phone. Like the computer mouse application, a number of measurements are taken to create a user template. Once enrolled, the user must repeat those gestures as a secondary authentication to gain access to an application or perform certain transactions.

### Biometric Solutions for Financial Services and Payments

Clearly, some of the biometric solutions reviewed above are not suitable for authenticating customers wanting to access financial applications or conduct payments. The suitability of those solutions that are in some level of usage today in terms of the factors detailed in table 2 have been evaluated by the author and are summarized in table 3 below.

[17] http://findbiometrics.com/biometric-signature-id-8212-ceo-jeff-maynard-announces-results-of-trial-using-gesture-biometrics-to-authenticate-student-id-with-the-university-of-texas-system-telecampus/

**Table 3: Biometric Solution Suitability for Payments**

| Biometric Method | Availability | Distinctiveness | Accessibility | Robustness | Acceptability | Financial |
|---|---|---|---|---|---|---|
| Fingerprint | High | High | High | High | Moderate | Moderate |
| Facial Recognition | High | Moderate | Moderate | Moderate | Low | Low |
| Iris Recognition | High | High | Moderate | High | Moderate–Low | Moderate |
| Hand Geometry | High | High | Moderate | High | Moderate | Moderate |
| Voice Recognition | High | Moderate | High | Moderate | Moderate | Moderate –High |
| Signature Scan | High | Moderate | High | Low | Moderate–High | Moderate |

As the table illustrates, none of the biometric methods evaluated scored perfectly across all the elements, with fingerprinting having the most number of "high" scores. Iris recognition and hand geometry followed closely.

### Device Fingerprinting

This technology combines the physical and biometric worlds for electronic devices such as mobile phones, desktops, laptops, and tablets, which generate specific data and electronic identifiers that allow for the creation of a profile or "fingerprint" of the device. While some of these identifiers, such as caller ID number or IP address, can be altered or spoofed, others are unique to the device. If the application has enrolled the device under a controlled environment, the device print can be used as an additional authentication factor (*something you have*) in a multi-factor authentication program. For example, when a customer communicates with a bank over a mobile phone, programs such as Pindrop Security can measure more than 150 factors[18] that are a combination of voice (*something you are*), device (*something you have*), and locational (*where you are*) identifiers to authenticate a caller. Combined with a user ID and password (*something you know*), such a system should provide an extremely high level of confidence in the authenticity of the user. Since it may take up to 30 seconds to obtain the complete set of identifiers, especially if a voice pattern has to be established, the application of this technology has to be carefully considered so as not to delay the customer's transactions.

While somewhat similar in concept, this method of authentication should not be confused with browser fingerprinting, which companies use to track a person's web browsing and access device characteristics (for example, screen resolution or fonts used). The subject of some controversy, this covert process is used to avoid the legal requirements related to "Do Not Track" opt-out

[18] www.pindropsecurity.com/phone-fraud-solutions/

options. While such tracking could be used as part of an authentication program, it is more commonly used for marketing purposes.

The growing inclusion of GPS functionality in electronic devices for mapping, navigation, and marketing applications is also being used for security applications. While not able to operate as a standalone authentication solution since it has information only about the device, which can be stolen, it can be combined with other authentication methods to help validate a user's location. This is particularly helpful in cardholder-not-present transactions.

### Out-of-Band Authentication

A recent development tied to the widespread deployment of mobile phones in increasing the confidence level that a company is dealing with the authentic customer is the use of out-of-band authentication (OOBA). In such a scheme, the customer is required to have enrolled an e-mail address or a telephone number with the company, information that the company has verified in advance of the transaction. Before a transaction is finalized, the company receiving the transaction request will send a message to the customer through a communications channel different from the one used to initiate the transaction. For example, if the customer is conducting business through an online banking site and wishes to initiate a wire transfer, the bank sends a code through a text message or e-mail that the customer must enter before the transaction is finalized.

As expected, the key to the success of this scheme is to have and maintain the correct phone number or e-mail address for the customer. For this reason, extreme care must be taken when enrolling the customer or when accepting any change to this information. Criminals have attempted to defeat OOBA systems in a couple of ways. One is to change the phone number or e-mail address on the account so the OOBA code is sent to the criminal instead of the legitimate customer. This can be done by social engineering techniques to gain initial access to the account to request the change. The most sophisticated efforts come from "man-in-the-browser" (MITB) malware. MITB malware is placed on the customer's device when the customer sees what appear to be authentic screens from the mobile banking application, but the Trojan installed on the device is intercepting the communication messages and allowing the criminal to execute an illicit transaction.

### Major Issues

**Card-Present (CP) versus Card-Not-Present (CNP):** In the payment card environment, the current network rules regarding whether the cardholder presents a physical card to an attendant is important in setting the merchant's interchange rate as well as liability responsibility. CNP transactions are riskier. Because the thief does not have to be physically present to execute a transaction, he or she often uses counterfeit or stolen cards through these merchant channels.

The 2013 Federal Reserve payments study[19] showed that the number of fraudulent CNP transactions was more than three times higher than fraudulent CP transactions. For this reason, CNP transactions carry a higher interchange rate and the merchant is generally liable for fraudulent transactions. This contrasts with the card-present environment, in which the financial institution issuing the payment card typically bears the liability for fraudulent transactions.

The evolving technology of payment form factors will create the need for the networks to examine their definitions of the CP and CNP environment. Electronic wallets have the cardholder load payment card information into an application resident on the mobile phone or tablet. The customer is physically present at the point of sale but uses the application to pay for the transaction. Is this a CP or CNP transaction? Under some of the card network rules, since the physical card was not processed, it is a CNP transaction. Under other rules, it is considered a CP transaction. As discussed above, the mobile application may actually provide more authentication capabilities than the standard card-processing environment, so shouldn't this additional risk-mitigation capability be taken into consideration?

**Privacy**: While the use of biometrics has a number of clear benefits in authenticating the legitimate user, their use and that of geolocation capabilities create consumer concerns about how the information will be used. Individuals have different privacy needs depending on the circumstances of their activity. In some cases, they essentially throw off any privacy needs when they engage in social media and other activities when their identity is clearly shown. However, even in such environments, there is some level of privacy desired, which became clear with Facebook's release of its 2013 annual report.[20] This report revealed that between 0.5 percent and 1.5 percent of its 1.2 billion active monthly accounts are false accounts established in violation of its service terms.

On the other end of the privacy spectrum, there are others who want to remain "off the grid" and disclose their personally identifiable information (PII) to others at an absolute minimum. Their primary concern is that their biometric data may be compromised in some way by criminals, or that their habits and movements will be captured and tracked by government entities, including law enforcement. Since biometric data is unique to the individual, it cannot be changed, so if it is compromised, the individual's ability to use that authentication method is stopped.

In table 4, below, the International Biometric Group (now Novetta Solutions) scored the various biometric authentication methods on their privacy risk level across four key attributes:

- Behavioral versus physiological: Industry risk experts believe that a physiological biometric such as a fingerprint or iris recognition is more likely to be used in an invasive manner.

[19] http://fedpaymentsimprovement.org/wp-content/uploads/2013_payments_study_summary.pdf
[20] http://investor.fb.com/secfiling.cfm?filingid=1326801-14-7&CIK=1326801

- Overt versus covert: A covert system is akin to being under surveillance without the subject's knowledge and is deemed to be more invasive.
- Verification versus identification: An identification system searches a large database of biometric templates (1: many), resulting in a greater potential for misuse, whereas a verification system is a 1:1 match decision.
- Existing database compatibility: If there are existing databases against which the template can be searched, the risk to the user's privacy is higher.

**Table 4: Privacy Risk Scoring**

| Biometric Method | Behavioral vs. Physiological | Overt vs. Covert | Verification vs. Identification | Existing Database Compatibility | Overall Risk |
|---|---|---|---|---|---|
| Fingerprint | High | Low | High | High | High |
| Facial Recognition | Moderate | High | High | High | High |
| Iris Recognition | High | Low | High | Low | Moderate |
| Retinal Scan | High | Low | High | Low | Moderate |
| Hand Geometry | Moderate | Low | Low | Low | Low |
| Voice Recognition | Low | Moderate | Low | Low | Low |
| Keystroke Scan | Low | Moderate | Low | Low | Low |
| Signature Scan | Low | Low | Low | Low | Low |

Source: Novetta Solutions (formerly International Biometric Group)

A biometric authentication program should include the following factors to help ease users' concerns about the use of their biometric data and their privacy.

- Transparency: The enrollment process as well as the ongoing operation of the program should be clearly explained to the user and, when appropriate, the user should be able to control the use of the data captured.
- Appropriateness: The data collected should be appropriate for the purpose intended.
- Purpose: The biometrics are used only for the purpose given and no other application.
- Security: The entity operating the program should ensure that careful enrollment and data protection safeguards are in place to prevent unauthorized access or unintentional disclosure.

**Other Risks and Controls**: In addition to the privacy issues discussed above, there are a number of other risk and control issues associated with biometrics.

- Enrollment: The enrollment stage represents a major point of risk, when the raw measurement data can be compromised or a false identity inserted. For this reason, there should be highly detailed procedures in place to ensure sufficient controls related to personnel and processes.
- Spoofing Attacks: If a biometric system is too simple, it is vulnerable to criminals who can spoof or fool the system by using artificial methods such as constructed finger or palm prints, photographs, or recorded voices. This risk is minimized by using techniques that verify that the subject biometric is alive—temperature, heartbeat, eye blinks, and more.
- False Templates: If the biometric templates are stored in a central database, controls must be in place to prevent the insertion of a template under another identity. The templates should be encrypted and there must be strong network and application security controls to restrict and track all changes to the application to ensure they are legitimate
- Data Interception: Just as in the point-of-sale world, the system must be designed so that the biometric authentication data cannot be intercepted between the reading device and the final creation of the template. End-to-end encryption is a best-practice solution.
- Component Alteration: Similarly, controls must be in place that will detect any hardware or software effort to modify the system outside the carefully controlled change process. Such alterations could involve the terminal capturing the biometric or an effort to manipulate the data on a template.
- Similar Template: The value of a biometric authentication system is it helps prevent fraudulent users from accessing the system if they have templates similar to authorized users. For this reason, the biometric system must be tested to ensure that its measurement and template algorithms are sufficiently complex to deliver unique outputs. The false acceptance rate of any biometric system should be less than or equal to 1 percent.[21]

[21] NIST Patriot Act Biometric Standard (http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2003-03/March2003-Biometric-Accuracy-Standards.pdf)

## Key Learnings

The research conducted for this working paper shows that there are a wide range of payment authentication methods in the marketplace today. As the number of remotely accessed financial applications increases, the need for additional authentication also increases to ensure the legitimacy of the person accessing the application.

Although many say the password is no longer viable, it is still the most used authentication method for access control and appears to be adequate by itself for routine, nonfinancial applications. What many people overlook with a password scheme is the long-term cost of password management in supporting the help desk function for users who forget their passwords. Passwords with additional authentication factors should suffice for the vast majority of financial service applications.

There is no single biometric method that is the “silver bullet” for providing a complete authentication solution for all applications. It is clear that multi-factor authentication schemes exponentially increase the confidence level of validating the proper user of an application. However, adding other authentication requirements potentially increases the amount of friction between the user and the service provider, with the possibility of causing the user to be dissatisfied to the point of abandoning the transaction and perhaps future transactions with that service provider.

The enrollment stage of the process is the most critical for making sure that the authorized individual is initially added to the application. Additionally, the application must have careful controls to guard against intruders gaining unauthorized access to steal or modify the stored authentication templates.

Due to the high penetration of smartphones in the United States, biometric efforts appear to be focused on fingerprint, facial, and voice recognition methods. Although embedded fingerprint sensors have only been introduced in the last few years, virtually all mobile phones contain cameras, and all contain a microphone.

While there may be some exceptions in the area of commercial banking, financial institutions will continue to carry the vast majority of the risk related to fraud losses with regards to consumer accounts.