Trusted Identities: Solving Fraud in Banking

One of the biggest challenges facing banks today is how to provide secure and trusted services while substantially improving customer experience. Fraud is an ever-present and increasing threat in an environment where bank customers are demanding a seamless and consistently satisfying experience across all service channels. These goals must be achieved without increasing cost or complicating the compliance process.

The answer is a holistic multi-channel identity and access management platform that correctly recognizes customers across all channels and uses biometrics to offer both a better user experience and a higher level of mutual trust. This approach also reduces complexity, vulnerabilities, and total cost of ownership. Biometrics is an essential component of this identity solution because it enables customers to conveniently and reliably prove that they are who they say they are — from account creation to any transaction.

Multiple Channels, Multiple Vulnerabilities

Today there is a patchwork of point solutions, each assembled and deployed separately, often by different organizations within the financial institution. The rush to meet customer expectations by offering mobile-relevant experiences has increased the dissonance. To individuals craving simplicity and a transaction environment they can trust, the fragmented experience is frustrating rather than empowering; to those seeking to defraud the bank and its customers, there are many new opportunities. Large-scale attacks where personal information is mined are increasingly more common and the information that is collected can be used to establish new accounts. Such identity theft has become more common as EMV has made card duplication more difficult.

The solution required is an integrated and mobile-relevant multi-channel identity and access management (IAM) platform that improves user experience and mutual trust at every point of contact, meets compliance requirements, reduces complexity, and lowers total cost of ownership.

Biometrics is an important and necessary component of this solution since it provides a means to prove or verify a claim of true identity — unlike something a person knows (e.g., a PIN) or something a person has (e.g., a card). This paper will explore how biometrics can be used to simplify IAM across all banking channels, improve user experience as well as the level of trust, and reduce total cost of ownership.

True Identity Matters

The concepts of identity and authentication have been blurred in the digital world. While each of us has a single, unique ***true identity***, most of us also have a plethora of digital identities such as an email address or username. These digital identities can be trivial to generate. When I click the "new user" button on the website of an online vendor, for example, I establish a new digital identity and associate a password — let's call this a credential. Thereafter, I present this credential to prove my ownership of the digital identity, and this process is called authentication.

Several problems arise here: 1) any person or entity that has possession of the credential can assume the digital identity, regardless of whether or not it is theirs; 2) there is weak to no binding of the digital identity or the credential to the true identity; 3) the means used to establish and validate the true identity are weak or nonexistent. These issues represent significant vulnerabilities to the concepts of identity and authentication and are some of the the reasons identity fraud and identity theft are a large and growing phenomenon.

How did we get here? Proving true identity has always been difficult and, because of that, methods to *approximate* proof of identity were created. These methods significantly increased convenience at the expense of trust. The first keyed door lock was invented 6,000 years ago because the alternative was posting a person who knew the true identity of the owner, by sight, at every door. The possession of the key replaced a proof of identity. In a sense, the key became a proxy for the owner's true identity.

In the computer era, the password provided a cheap, acceptably convenient proxy for one's true identity, albeit a very weak one. Then, as we entered the connected era, this weakness could be exploited *en masse*. In response to this threat, password complexity and expiration rules destroyed convenience, with little if any reduction in fraud vulnerability.

Fortunately, technology has evolved and today we have the means to eliminate identity theft and fraud. However, the solution requires an integrated approach in which a chain of trust is established and maintained in a way that delivers the required level of security in a manner that is cost-effective and convenient.

Machine-verified biometrics plays a critical role in delivering this solution because only biometrics can directly reference a person's ***true identity***. Indeed, biometrics provides the only means to unambiguously validate an identity claim, and it can do this while eliminating the cost, complexity and inherent vulnerabilities of passwords and other methods that merely approximate proof of true identity.

The Promise of Biometrics, Theory and Practice

In order to eliminate identity theft and fraud it is imperative that we distinguish between 1) the use of biometrics as an authentication factor or credential to prove a claim of digital identity ownership,

and 2) the use of biometrics to prove a claim of true identity. The real value of biometrics is making the verification of a claim of true identity at least as convenient as using a credential to verify a claim of digital identity ownership AND delivering that verification at a higher level of trust.

Let's consider the example of biometrically-enabled smartphones. Today a person can purchase such a device with a credit card and a billing address, and bind the device to an email address and password. A device PIN or password is created, and the PIN or password is used to capture a fingerprint biometric on the device. This device can then be associated with multiple payment accounts and, in turn, each account can be associated with the captured fingerprint biometric.

The result is a convenient way to perform "card not present" (CNP) transactions both online and at the retail point of sale. In this smartphone scenario, ***the fingerprint biometric was not used to verify a claim of true identity*** — it was simply used as a credential to replace a PIN or password. The transaction is certainly more convenient, but trust is significantly lower than for an in-person transaction with a card. Mobile-based CNP transactions are clearly a preferred method of payment by consumers and are poised to replace transactions where the card is presented in person. But, not surprisingly, CNP fraud is on the rise — and the on-device biometric cannot prevent it. What is needed is an unbroken chain of trust for transactions that are based on verifying a claim of true identity, rather than simply verifying ownership of a digital identity that someone might be using fraudulently.

True Identity and the Chain of Trust

Consider an alternative approach to the traditional process of simply verifying digital identity ownership. A person is identity-proofed at a NIST Level of Assurance[1] 3 or 4 and the entity performing the identity vetting captures biometrics data from the individual. In other words, true identity is established and verified at the very beginning. An ID based on this true identity is issued by the identity-proofing party, and the biometrics of the person that was identity-proofed are embedded in a physical ID card or its digital equivalent. The ID proofing entity could be a government agency, bank, or independent identity provider (IDP). Subsequently, when a mobile device or SIM card is purchased, the purchaser presents the identity-proofed ID and uses the validated biometric to prove that the person in possession of the ID is who he or she claims to be.

Now imagine opening a banking account with that mobile device, or even conducting a CNP transaction. This strong association of a person's true identity to account creation, and subsequently to each transaction, delivers a high level of trust in a manner that is very resistant to identity fraud and theft.

Working with identity proxies rather than true identities is certainly easier: Establishing and maintaining a chain of trust involves incremental expense in the identity proofing process, may

[1] NIST SP 800-63 Electronic Authentication Guideline establishes rules for identity proofing an individual at one of 4 levels of assurance (LOA1 – LOA4). The higher the level the stronger the proof is that the person is who they claim to be.

require the services of an IDP, and depends on a trusted electronic means of conveying the ID. Plus, the biometric device that is used to prove that the person in possession of the credential is actually the person that was issued it must now be interoperable, meaning independently verifiable. Current mobile device fingerprint readers, for example, are not capable of this.

However with this alternative approach — establishing true identity in a manner that can be independently verified not only at account creation but at each transaction — identity theft and fraud can be eliminated. To realize this vision, the cost of ownership needs to come down and the level of convenience needs to improve. We also need to shift our attention from authentication factors and PINs and other secrets to a focus on the viable ecosystems that can now support the establishment of true identity and the proof of a claim of true identity.

What's Next

The financial industry is at the forefront of implementing biometrics. HID Global's Lumidigm biometrics solutions are a big part of this adoption curve, with more than 81 million Brazil bank customers using fingerprint biometrics to authenticate at over three billion ATM transactions in 2016 alone. To fully realize the short- and longer-term benefits of biometrics, however, there must be an integrated platform that recognizes true identities from establishment to authentication — a chain of trust. IAM solutions will greatly improve the customer experience while increasing trust and lowering costs if they include mobile-relevant, multichannel-capable identity and access management approaches that are secured end-to-end and are easy to buy and to deploy.

Moving forward, there is also the opportunity to deliver a game-changing user experience across all banking channels, leveraging new methods that are contextually aware, continuous and truly seamless. By combining multiple types of biometrics with mutual authentication, mobile certificates, deep learning and other technologies, banks will be able to create an environment in which there is no explicit requirement that the user do anything other than "show up" for his or her transaction on the phone, at the bank or teller machine, or online.

As these integrated platforms, biometrics solutions and related technologies are adopted, they will better position the banking industry to improve customer experience and reduce fraud and the cost to serve. They will also lay the foundation for replacing the verification of an identity proxy with the verification of a true identity. When verifying a claim of true identity becomes as convenient as verifying a credential is today, we will have come a long way in reducing the threat of identity theft and identity fraud.

2017-04-26-17-hid-biometrics-banking-fraud-wp-en PLT-03315