Digital Identity In Banking

What CEOs Need to Know About Best Practices and Future Directions

RON SHEVLIN
Director of Research
Cornerstone Advisors

CORNERSTONE
ADVISORS

TABLE OF CONTENTS

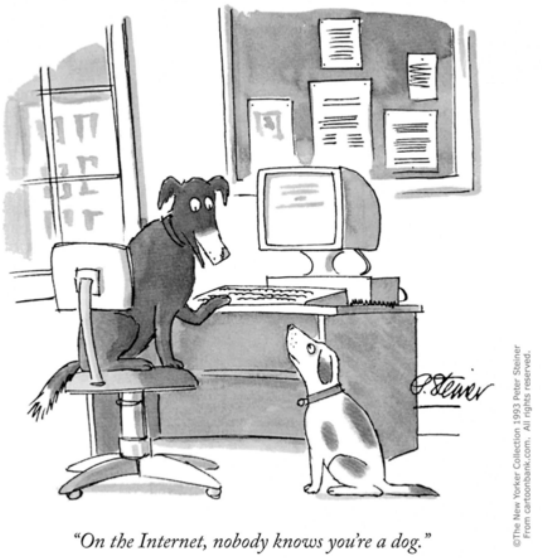
DIGITAL IDENTITY:
A CHALLENGE AS OLD AS THE INTERNET

Although the topic of digital identity gets daily attention today in 2018, it's hardly a new topic. In 1993, *The New Yorker* published what has become one of the most—if not the most—iconic cartoons about the Internet (Figure 1). In it, one dog says to another, "On the Internet, nobody knows you're a dog."

Twenty-five years ago, many people saw the ability to remain anonymous as a *feature* of the Internet, not a liability. Despite a quarter century of technological advances that include e-commerce, social media, and the smartphone:

> *"There is still no easy way to prove online that you are not a dog, are over 18, live at a certain address, graduated from a certain school, work at a specific company, or own a specific asset. These kinds of assertions about ourselves are difficult to trust because they are nearly impossible to verify."* [1]

FIGURE 1: **New Yorker Cartoon on Digital Identity**


P. Steiner
"On the Internet, nobody knows you're a dog."
©The New Yorker Collection 1993 Peter Steiner
From cartoonbank.com. All rights reserved.

Source: *The New Yorker*

WHY IS DIGITAL IDENTITY STILL A PROBLEM?

If we've seen 25 years of technological advances, then why is digital identity still a problem? Three reasons: 1) There are no standardized formats for digital credentials; 2) There are no standardized methods to verify the source and integrity of digital credentials; and 3) The technological advances that *have* occurred over the past 25 years have exasperated the problem—not alleviated it.

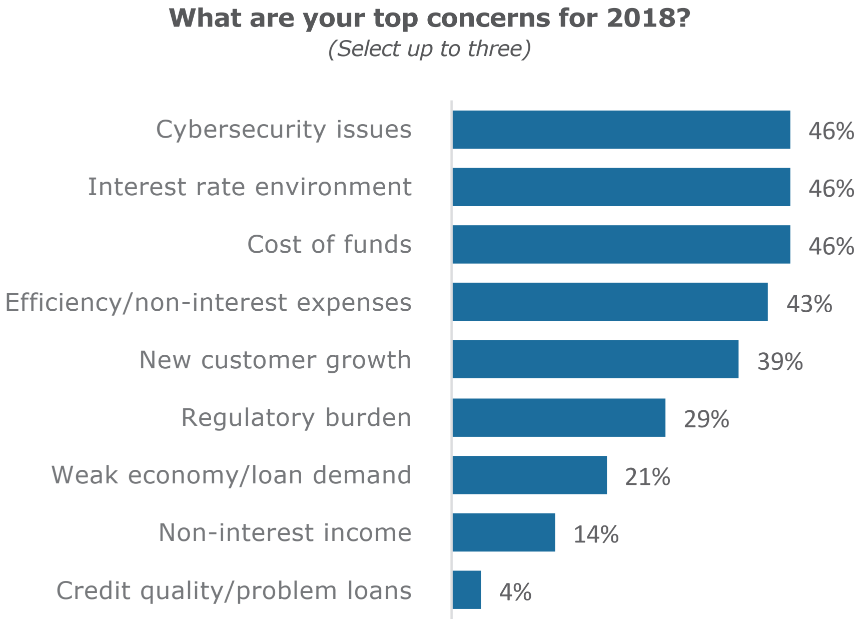
The meteoric growth in smartphone adoption over the past 10 years outstripped any industry's or government's ability to address digital identity challenges. The emergence of distributed ledger technology (e.g., blockchain) promises new approaches to digital identity management, but is emerging relatively late to the game. And with the rise of the Internet of Things (IoT) comes a new reality in digital identity: "On the Internet, no one knows you're a refrigerator pretending to be a dog."[2]

WHY HAVEN'T BANKS DONE SOMETHING ABOUT DIGITAL IDENTITY?

A combination of factors has kept U.S. banks from attacking the digital identity situation. Consumer adoption for digital access to bank accounts in the United States has lagged other industries and countries. Twenty years after banks began to provide online banking, only about two-thirds of Americans access their accounts online, and only about a third have access through a mobile device. Complicating the picture, the regulatory environment has shielded consumers from fraudulent activity. As a result, banks have felt little pressure from consumers or regulators to address digital identity concerns.

Until now. Bank execs are ready to act on digital identity issues. When asked about their concerns for 2018, bank CEOs ranked cybersecurity at the top, tied with interest rates and cost of funds (Figure 2).[3]

FIGURE 2: **Bank CEO Concerns**



Source: Cornerstone Advisors survey of 262 bank and credit union senior executives, Q4 2017

What's the path forward? This report will explore three avenues: 1) Technology developments in digital identity management; 2) Best practices in digital account opening and authentication; and 3) Forces shaping digital identity management.

TECHNOLOGY DEVELOPMENTS IN DIGITAL IDENTITY MANAGEMENT

Experienced bankers understand the maxim "new banking channels emerge, but old channels never die." Identity management is similar: New methods for identification emerge, but old authenticators don't go away. Traditional authenticators include what a person *has* (access badge, identification document) and *knows* (password, PIN, secret fact).

Technological advances over the past quarter century have added two biometric-based categories of identity authentication: What a person is (voice, fingerprints, face) and *does* (keystroke activity, device usage) (Figure 3).

FIGURE 3: **Identity Authenticators**

		PHYSICAL BIOMETRICS	BEHAVIORAL BIOMETRICS
WHAT A PERSON **HAS:**	WHAT A PERSON **KNOWS:**	WHAT A PERSON **IS:**	WHAT A PERSON **DOES:**
Access badge **ID document** **Smart card** **Security token** **Mobile phone**	**Password** **Passphrase** **PIN number** **Sequence** **Secret facts**	**Fingerprints** **Facial images** **Iris image** **Vein images** **Voice prints**	**Keystroke activity** **Device usage** **Channel behavior**

Source: Accenture

PHYSICAL BIOMETRICS

The various forms of physical biometrics have strengths and weaknesses:

Voice Voice recognition is minimally intrusive to the user experience and applicable to a wide range of devices. The downside, however, is that it's subject to false positives due to ambient noise and susceptible to spoofing by replaying a recorded voice.

Face Consumers are familiar with, and comfortable taking selfies. Two-dimensional facial recognition provides decent security if used in conjunction with a fingerprint, and excellent security if three-dimensional technology is used. The technology is susceptible to variations in light, pose, expression and facial appearance, however, and spoofing is possible with two-dimensional approaches.

Fingerprint The ubiquity of fingerprint recognition on smartphones (expected on 100% of devices by 2020) makes this approach well-accepted among consumers. But fingerprints can be difficult to read with wet or rough fingers, and scanners are susceptible to spoofing.

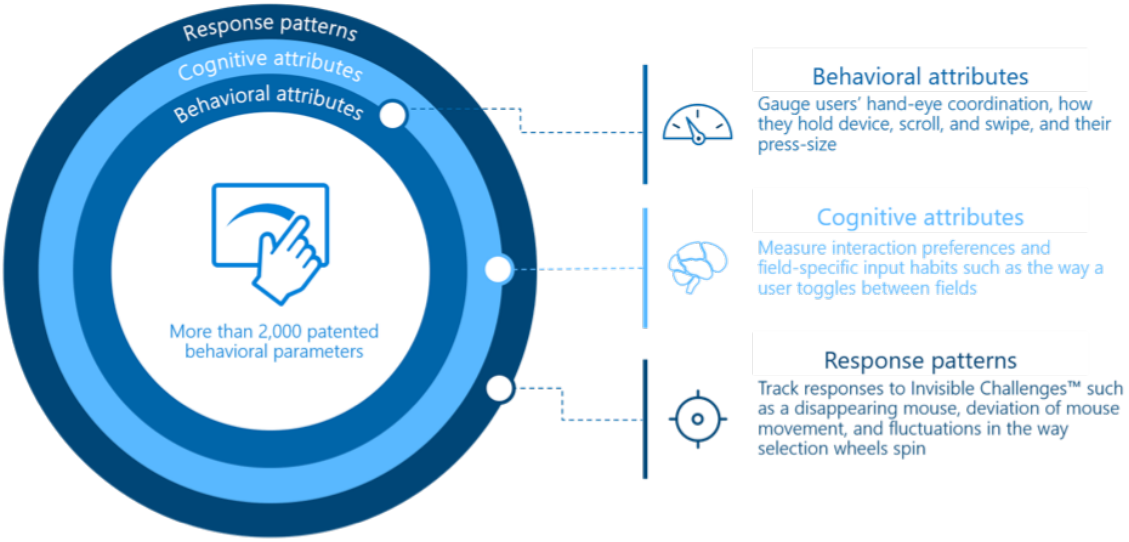
Iris Iris recognition (there's no such thing as iris "scanning," by the way) provides a higher level of security than facial recognition or fingerprints because of the difficulty to spoof. But it requires special hardware, and it doesn't work particularly well in sunlight, with people who wear glasses, or with people who have eye conditions like cataracts.

Vein Recent studies claim that the accuracy of vein readers (looking at palm veins) is as good as iris recognition.[4] In addition, the medical community is getting on the vein train because it's found that vein recognition is effective with unconscious patients (generally not a problem in banking, but you never know). The current downside to this approach is the high cost of readers.

BEHAVIORAL BIOMETRICS

Although behavioral biometrics isn't new—the measurement of patterns relating to human activity dates to the 1860s—it has garnered increasing interest in the past few years. This approach evaluates how people interact with their devices, including typing speed and patterns, and even how they hold the device (Figure 4).

FIGURE 4: **Behavioral Biometrics**


Response patterns
Cognitive attributes
Behavioral attributes
More than 2,000 patented behavioral parameters
Behavioral attributes
Gauge users' hand-eye coordination, how they hold device, scroll, and swipe, and their press-size
Cognitive attributes
Measure interaction preferences and field-specific input habits such as the way a user toggles between fields
Response patterns
Track responses to Invisible Challenges™ such as a disappearing mouse, deviation of mouse movement, and fluctuations in the way selection wheels spin

Source: BioCatch

Behavioral biometrics is useful for detecting an account takeover (ATO) and new account fraud. According to Aite Group:

> *"Behavioral biometrics serve as an early red flag by detecting deviance from the user's normal interaction patterns. Fraudsters input data differently than genuine consumers—they don't have the same level of familiarity with the data, so they're more likely to repeatedly delete and fix typos. Criminals are also more likely to copy and paste data (pulling it from a data dump purchased off the dark web), and they will have more familiarity with the application layout given their frequent use, which manifests in a much different rate and pattern of interaction than a genuine consumer."*[5]

U.K.-based National Westminster Bank (NatWest) has deployed behavioral biometrics tools that build a unique biometric profile for each customer and conduct comparisons against it each time the user logs in to the bank's mobile app or online banking site. According to the bank's director of innovation:

> *"Behavioral biometrics are especially good at recognizing the work of malware such as remote-access Trojans. Machine-automated behaviors bear no resemblance to human behaviors. [And] it provides an ability to alert and prevent fraud taking place as opposed to helping you detect or correct after the event."*[6]

SO WHAT

In practice, behavioral biometrics are more effective for proving that the user isn't who he or she claims to be than proving that the user is who he or she claims to be.

Because there is no physical biometric element captured, behavioral biometrics are transparent to end users and generally not subject to regulatory scrutiny. One downside, however, is that it is JavaScript-intensive, requiring tags on every webpage. Critics point to other drawbacks:

> *"As soon as somebody manages to build a biometric profile of your keystrokes at a network/website where you are otherwise completely anonymous, that same profile can be used to identify you at other sites you're using. With keystroke dynamics applied, advertisers could identify you without using any of the current tracking technologies."*[7]

USER DATA VERIFICATION

Banks have long relied on the large credit bureaus to validate customers' and prospects' personally identifiable information (PII). After the Equifax breach of 2017, however, questions arose regarding the viability and wisdom of relying on the bureaus.

At a closed session of senior retail banking executives at an industry conference not long after the Equifax incident, the chief retail banking officer at a Top 10 U.S. bank was asked if his bank would continue to use Equifax. His reply: "Sure. Who else are we going to use?"

New data sources are emerging—if not to replace the bureaus, at least to supplement them.
These sources include:

Document capture Solutions from market leaders like Mitek use the smartphone's camera to take a picture of an identity document (e.g., a driver's license or utility bill), verify the credential, and parse the data into an onboarding system. Many solutions validate that the document is genuine, and some include an automated feed to an identity data element verification solution.

Mobile device ownership

As smartphone adoption becomes ubiquitous in the United States (two-thirds of consumers between the ages of 55 and 75 have smartphones), the device becomes an increasingly important tool in ID verification beyond capturing biometrics. According to Aite Group, "real-time interfaces with mobile network operators enable positive verification that the device belongs to the person authorized on the mobile account and provides notification if the device is lost or stolen. It also provides risk indicators about the account, e.g., whether the number was recently ported, and how long the account has been in existence."[8]

Social media

With the widespread adoption of social media platforms, data from a platform like LinkedIn provides strong clues about whether people really are who they say they are. Critics of this source of data will point to the ease of faking a social media account. That may be true, but a good social identity solution will look at the age of the account, the depth of data, how much the account interacts with other accounts, consistencies between that account and other connected accounts, as well as text analytics to confirm that the account is genuine and that the information provided is real.

Suspicious identity

Suspicious identity lists include identifying data elements that have been previously associated with fraud that provide an early warning of high-risk activity, for example if an identity or device is being used to open multiple accounts simultaneously at multiple providers. A variant on the concept are dark-web crawlers, which monitor underground websites looking for payment card or identity data for sale.

FIVE FORCES SHAPING DIGITAL IDENTITY MANAGEMENT

Where is digital identity management going in the next five to 20 years? Five forces are influencing the direction of digital identity management: 1) Device- versus cloud-based identity management; 2) Identity platform providers; 3) Internet of Things; 4) Blockchain; and 5) Geopolitical trends.

DEVICE- VERSUS CLOUD-BASED IDENTITY MANAGEMENT

One of the debates raging in the industry is where should digital identities be managed—on the device, or in the cloud (i.e., the server)? The alternatives involve:

- **Device-centric architecture.** The analysis, biometric template creation, storage and matching all occur locally on the device. In a FIDO ("Fast IDentity Online")-compliant system, a successful biometric match grants access to a private key stored on the device, which is in turn used to respond to a PKI (public key infrastructure) challenge from a relying party, such as a bank or retailer whose app is running on the device. The private key never actually leaves the mobile device.

- **Server-centric architecture.** In this setup, the biometric template is enrolled and stored centrally in a secure server. Matching and liveness-detection upon an authentication attempt are performed centrally, as opposed to on each individual device.[9] Each time the user performs a verification attempt, the captured sample is sent to the central matching engine, where it is processed and matched against the enrolled template stored centrally.

Each approach has its advantages. Although there are more issues, or factors, impacting the choice between device and cloud than those listed in the table, the debate has no clear winner (Table A).[10]

TABLE A: **Advantages of Device Versus Cloud-Based Identity Management**

	ADVANTAGE		RATIONALE
Issue	Device	Cloud	
Large-scale data breaches	✓		Single breach of central storage location exposes many more locations
Perimeter defense		✓	Central storage means smaller, easier-to-defend perimeter
Lost or stolen devices		✓	Server segregates biometric data from other PII
Man-in-the-middle attacks	✓		Biometric templates less vulnerable to interception
Validation and matching		✓	Biometrics used as part of ID proofing and other processes
Scalability	✓		Processing and storage distributed across devices
Data analysis		✓	Aggregated data available for improved algorithms
Bandwidth/data consumption	✓		Faster authentication, less data transmitted to server

Source: Aware

Proponents of the cloud-based approach argue that it:

- **Always distinguishes individuals.** It creates a direct biometric link between an individual and their UVI providing a secure and reliable level of identity assurance.
- **Prevents password or PIN workarounds.** According to Acuity: "For the current generation of mobile devices, biometric authentication is a convenient password or PIN overlay, not the foundational device security biometric. Authentication as foundational security will significantly improve the reliability of the link between the user and their device, but It will not provide additional identity assurance for cloud applications."
- **Enables enrollment of multiple biometrics from a single device.** Proponents claims that a cloud-based approach will provide dynamic, universal, cross-channel access to digital services across applications and devices.

In addition, the pro-cloud camp often points to various shortcomings of device-based approaches, which often have a flip-side counterargument (Table B):

TABLE B: **Shortcomings of Device-Based Biometrics**

ISSUE	SHORTCOMING	COUNTERARGUMENT
Lack of portability	Device-based biometrics aren't portable and can't be backed up	They can't be hacked or stolen
Device variability	Interfaces vary across devices and enrollment on each device is required	Consumers may prefer this and see it as a benefit, not a drawback
Cross-channel identity	Can't easily maintain unique cross-channel identity	
Multiple identities per device	Multiple individuals can enroll on a device with no way to know whose biometric is being used to approve a transaction	Spouses, partners and/or family members may share a device and have a valid need to maintain multiple IDs on a single device

Source: Cornerstone Advisors

SO WHAT

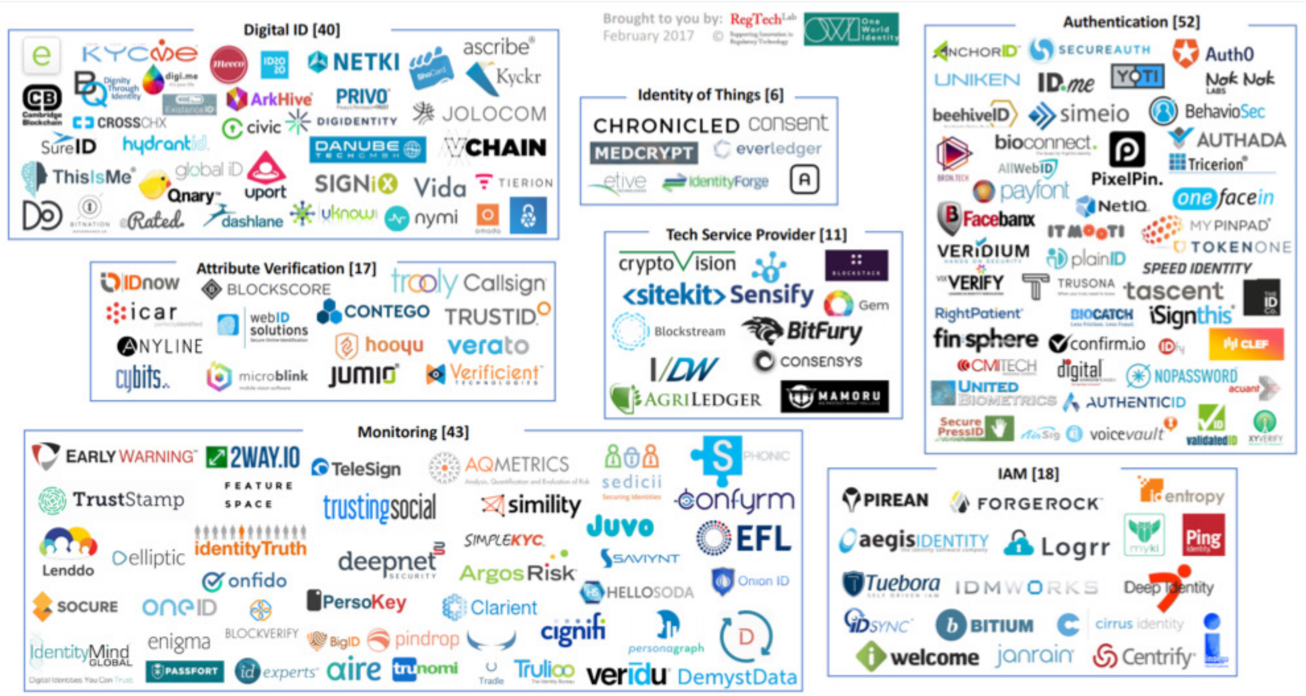
Critiques of individual physical biometrics and device-based approaches stem from a desire to find a silver bullet that will provide the one perfect solution to digital identification. Since that's not feasible, many FIs employ a multi-modality approach, combining physical biometric approaches. But as new biometric approaches emerge—DNA analysis, vein analysis, earlobe geometry—the costs and complexities of digital identity management will rise, not decrease.

While each approach has its advantages, all factors aren't necessarily evenly weighted. It's hard not to tip the scales toward giving people control over their own individual data, especially considering the Equifax breach and the Facebook controversy involving Cambridge Analytica. According to PwC, "Individual choice and control means that the individual [can] withdraw permission to use their data at any point; this is simpler where biometric data is stored on a local device as the individual has far more control over the data because they can just delete it. In addition, authentication systems based on the FIDO authentication protocols allow the user to revoke permission at any point by de-registering from the service." [11]

IDENTITY PLATFORM PROVIDERS

As digital identity technologies have evolved over the past 10 years, vendors in the space have multiplied like rabbits. One World Identity's (OWI) vendor landscape map lists more than 225 firms in 13 different categories including biometrics, fraud and identity protection, identity and access management, and KYC/AML compliance.[12] A separate analysis from Pascal Bouvier from Santander InnoVentures identified nearly 190 startups across seven of OWI's categories (Figure 5).[13]

FIGURE 5: **Identity Management Vendor Landscape**



Source: Pascal Bouvier

SO WHAT

The complexity of deploying and integrating digital identity management solutions will lead to the emergence of identity platform providers (IPPs) that will simplify the vendor selection and management challenges facing financial institutions. These platforms will enable providers across the identity ecosystem to easily integrate and, just as importantly, extend their marketing reach. Various models of IPPs exist and are emerging, each with their own risks and drawbacks (Table C).

TABLE C: **Identity Platform Provider Models**

TYPE	DESCRIPTION	EXAMPLES	PRIMARY RISK
Monolithic Identity Provider	Single universal identity scheme	Facebook Google	Sharing of personal data with malicious or unaccountable third parties
Federated Internet Identity Provider	Like Monolithic model, but providers are less dependent on profiling users to monetize personal data	GSMA Mobile Connect Open ID Connect Mobile Operators PayPal Amazon	Sharing of personal data with malicious or unaccountable third parties
Brokered Identity Provider	Provides governments with a means to establish a marketplace for digital identity services	UK Verify US Connect.Gov	Hub architecture provides point of aggregation
Brokered Credential Service Providers (CSP)	Establishes reliable authentication credentials that can be used to assert an already established identity	Canada Credential Broker Service	Hub architecture provides point of aggregation
Personal Identity Provider	Makes citizens the gatekeepers of their data, providing high level of control to the individual	Mydex Meeco Microsoft U-Prove	Consumers may be unable to effectively manage personal information

Source: Consult Hyperion

Could banks emerge as identity platform providers? According to identity expert Dave Birch:

> *"For banks to proactively create a new set of identity services would not be that far removed from what they are required to provide today to comply with KYC [Know Your Customer] and other regulations. It would also offer a welcome opportunity to strengthen customer relationships and encourage customer loyalty at a time when other aspects of the banking business are being disrupted."*

The World Economic Forum writes:

> *"There is a strong business case for financial institutions to lead the development of digital identity systems [that include] opportunities to: 1) Streamline current processes, increase automation, and reduce error and human intervention; 2) Create new revenue streams from new products and services; and 3) Stretch outside of core business and capabilities to create transformational new business models and reach new customers."*[14]

In addition, a BBVA Research report on digital identity lists reasons supporting the "bank as identity provider" argument.[15] And, of course, there are counterarguments (Table D).

TABLE D: **Banks as Identity Providers**

FACTOR	ADVANTAGE (PER BBVA RESEARCH)	COUNTERARGUMENT (PER CORNERSTONE)
Experience	Banks have already designed secure processes to verify customer identities and will be able to offer services to other industries, especially in terms of onboarding individuals, assets and institutions onto digital systems.	From a U.S. perspective, only four or five banks have the scale to do this. Credit unions might be able to band together to create a Credit Union Service Organization (CUSO) to provide these services.
Trust	The higher the level of assurance providers have, the more important the transactions they can do. After public providers, banks are the most reliable private sector providers.	Many consumers do trust banks to store and share their data responsibly.[16] But does this not translate to identity management, an unknown concept to consumers?
Compliance	Banks are used to dealing with compliance standards and can offer their expertise in identity-based networks.	A competency in complying with bank regulations shouldn't be confused with a competency in complying with new and emerging identity regulations.

Source: BBVA Research, Cornerstone Advisors

SO WHAT

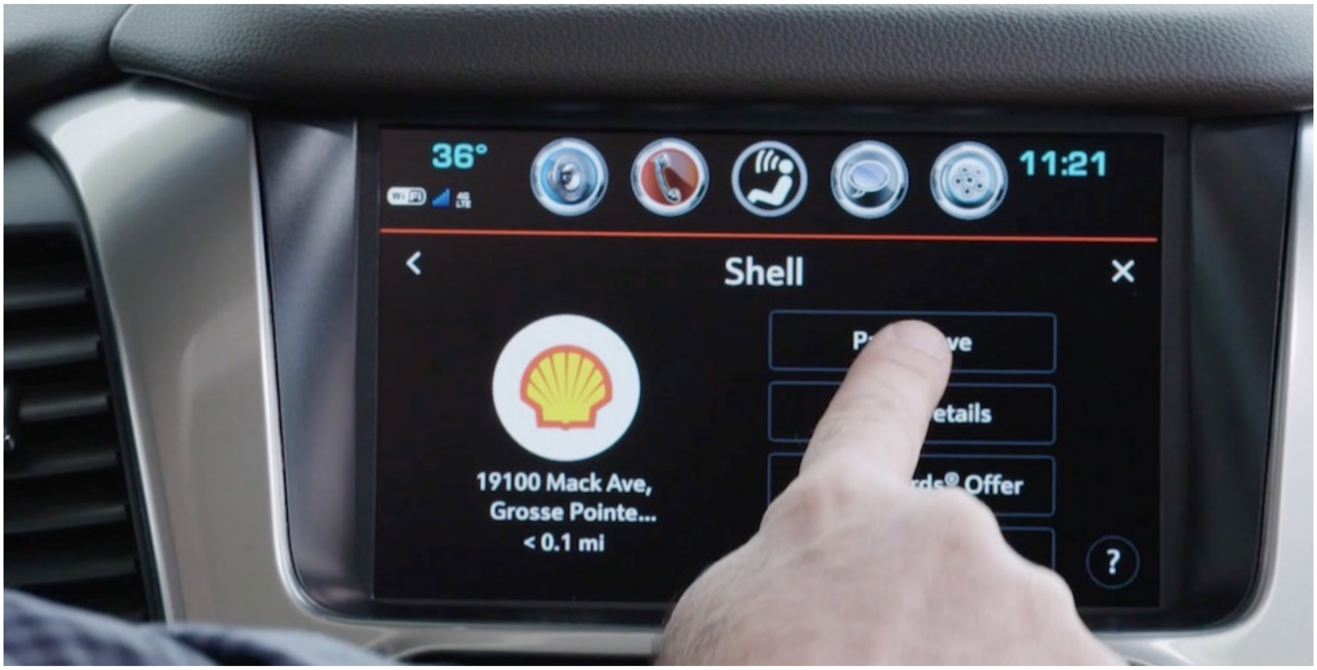
The flaw in the "banks as identity provider" argument is that there is no rationale for multiple banks to compete to be *the* primary identity provider. When someone switches banks, does that mean that his or her identity credentialing will have to shift from one provider to another? It's enough of a hassle to switch banks, can you imagine the hassle of having to switch identity providers when you change banks?

INTERNET OF THINGS

Estimates of the number of devices that will be connected to the Internet in 2020 range from 20 billion to 75 billion. Whoever's estimate is closest will get their bragging rights, but for bank execs, the actual number doesn't really matter. What matters is that some of those devices are going to want to access information about their owners' bank accounts and make payments, and that presents a whole new world of identity management issues that financial institutions have never dealt with before.

This isn't some future fantasy. In February 2017, Jaguar announced that it was working with Shell to enable its U.K.-based car owners to use Apple Pay or PayPal to pay for gas from within their vehicles at the pumps.[17] And in April 2018, Shell announced it was teaming with Chevrolet to allow drivers to pay for gas from their vehicles' infotainment screen (Figure 6) [Author's note: If you still have to get out of the car to pump the gas, is paying from inside the car that big of a convenience?].[18]

FIGURE 6: **In-Car Gas Payments**



Source: PSFK

The intersection of digital identity and the Internet of things (IoT) will produce numerous decision-making challenges for bank executives:[19]

- **Adaptive authentication.** Authentication requirements vary for different types of device. A smart refrigerator may require one (relatively simple) method of authentication, while an autonomous car, with multiple drivers and users, will require a higher security threshold.

- **Privacy and preference management.** Bank customers will need three privacy-related capabilities: 1) Enabling customers to self-manage preferences such as opting in or out of communications and granting their consent for data sharing; 2); Setting notification alerts based on user preferences; and 3) Aggregating customer preference data captured from different interaction points into a single profile.

- **Policy-based data access governance.** With traditional identity access management approaches, IT teams can grant access to data based on job roles and titles. However, in IoT use cases, data access must be attributed more granularly to individual devices, applications and users. Policy-based governance controls are needed to apply access on different levels and contexts. For instance, data access can be granted or denied according to IP address, industry or geographic regulatory constraints, time frames, corporate mandates and individual customer consent, among other criteria.

BLOCKCHAIN

Many identity experts foresee the application of blockchains to identity management. Numerous startups have launched identity registration solutions using distributed ledger technology, while others are developing new blockchain-inspired infrastructure for distributing attributes, a key element of identity management. As with everything else in the world of digital identity management, there are two sides to the coin:

- **Pros.** One advantage of blockchains, especially the public instances, is discoverability. Their distributed nature and transparent, open source software, installed across the world, means that finding records is straightforward and requires no central directory or addressing scheme.

- **Cons.** Additional privacy controls are needed, for example: 1) Separately encrypting transaction payloads before they're slotted into or referenced from blockchain entries; and 2) Creating extra access control layers to restrict who can read from (or write to) the ledger.

What should bank execs be concerned about *today*? The evolving use of blockchains to manage digital identities will require resolving challenges like:[20]

- **What should be done off-chain?** Determining which identity data is pertinent, who vouches for it, and how to keep it current may involve third parties or authorities that may not utilize distributed ledger technology.

- **How will banks protect private key safety?** Once it became apparent that bitcoin private keys could be lost or stolen by hackers, new solutions emerged, including cloud-based key stores, mobile phone storage, backup services, and personal hardware security modules.

- **Who maintains the chain?** One concern for blockchain-based identity management is who performs software maintenance. When bugs or urgent design improvements arise, banks will want certainty as to when fixes will be deployed, which is not the current case with open source volunteers providing maintenance. A bug in Ethereum led the founder to “fork” that blockchain, leading to multiple incompatible records and variations of the currency. It’s hard to imagine any bank or credit union (or regulator, for that matter) accepting that situation.

The global head of digital banking at a $1 trillion bank believes blockchain for digital identity isn’t too far away, but sees some challenges:

> *“Banks like Rabobank and RBS have done proof-of-concepts that address actions, consent, and decentralize commitment. But they haven’t stored the identities—that’s what needs to be solved. Blocks take time to create. The biggest barriers are liability and trust. Do banks trust each other? Can the first entity be trusted? Can we trust others to have the same stringent KYC policy that we do?”* [21]

Organizations leading the development of distributed ledger-based digital identity solutions include:

- **R3.** This consortium of banks and other firms has developed Corda, a distributed ledger platform to record, manage and synchronize financial agreements between regulated financial institutions. In November 2016, R3 announced that it was testing a distributed ledger-based know-your-customer registry. In January 2018, it announced an agreement with Evernym, a blockchain identity solution running on the Sovrin distributed ledger platform.

- **CU Ledger.** This 80-credit-union consortium is investigating the viability of a private, permissioned distributed ledger for credit unions. In February 2018, it too announced a partnership with Evernym to launch MyCUID, a consumer-focused digital identity solution. The service is intended to provide credit union members with a way to control their personal identifiable information. As reported in TearSheet, its first application will identify members when they use call-center services, with pilots expected to be launched in the second half of 2018.[22]

- **Sovrin Foundation.** The Sovrin Foundation is a private-sector, non-profit organization established to govern the world’s first self-sovereign identity (SSI) network. In 2017, Sovrin transferred the open source code base—originally contributed by Evernym—to the Linux Foundation to become the Hyperledger Indy project.

GEOPOLITICS

Various governments around the world have launched identity initiatives including:[23]

- **Austria.** Austria’s Citizen Card is designed to provide a secure and privacy-friendly form of identity management. The critical technological feature of the Citizen Card that makes it a good model for emulation is the use of un-linkable sector specific identifiers (and associated cryptographic keys and digital certificates). Positive aspects of the approach include: 1) Comprehensive data protection law; 2) Independent data protection authority; 3) Limited data kept on the card; 4) Separation of identities by sector; and 5) Integration with 12 government services. Drawbacks, however, include concerns about the security of card readers.

- **Estonia.** The Estonian e-ID card includes an embedded PKI application that enables online authentication and digital signature with electronic certificates. More than 600 online government services are available through the use of the online authentication system; companies have access to more than 2,400 services. In the past decade, no security breaches have been reported. Positive aspects of the system include: 1) Comprehensive data protection law; 2) Independent data protection authority; 3) Logging that enables auditing; and 4) Minimal data is provided to service providers. The drawback is that excessive data is held on the card.

- **United Kingdom.** GOV.UK Verify is an identity scheme that establishes a private sector marketplace for digital identity, with private sector organizations creating and managing digital identities on behalf of citizens. Positive aspects of this approach include: 1) Comprehensive data protection law; 2) Independent data protection authority; 3) Decoupling of identity providers and service providers; 4) Minimization of data sharing; and 5) Focus on end-user experience. Drawbacks include the potential for tracking and surveillance to occur as a result of "matching data set" in all identity transactions.

SO WHAT

Or more specifically…so what about the United States? The prospects for a digital identity scheme in the United States on par with what Austria, Estonia or the United Kingdom has done look slim for the short-term. Today's political climate will squelch any national identity effort, which will be seen by many (on one side of the political spectrum) as an attempt to limit immigration and identify (and remove) immigrants illegally in the United States. In addition, a government-driven identification system hardly seems to be a priority to the other side of the political spectrum.

As a result, the United States is destined to play catch-up with—and be impacted by—the rest of the world. European developments like GDPR impact U.S. banks and, in some cases, conflict with U.S.-based law—for example, the requirement to notify the government of a data breach within 72 hours of its discovery.[24] According to Andy Roth, partner at law firm Cooley LLP:

> *"A European data subject can make requests on what data the bank has on it and can make changes and request deletion of the data. These require business practices that banks don't have in the U.S."*[25]

While the United States fiddles around with what to call the Consumer Financial Protection Bureau (the current director claims the legal name is Bureau of Consumer Financial Protection, and there's a bill in the House to change the name to the Financial Product Safety Commission), Rome is burning—the U.S. banking system, that is. Meanwhile, digital identity issues go unaddressed.

BEST PRACTICES IN DIGITAL IDENTITY MANAGEMENT FOR TODAY

A white paper from a fintech vendor recently crossed our desk, in which the author wrote, "The first step to a mobile-first strategy for banks is to provide a frictionless experience." It reminds us of the old Steve Martin routine on how to become a millionaire: "First ... get a million dollars."

Providing a frictionless experience isn't anybody's first step—it's the objective or goal. Getting there is hardly an easy task. From our interviews with leading financial institutions, we've identified best practices in authentication and digital identity management that balance the need to reduce fraud but create a good user experience:

- **Evaluate the source of the application.** How did an applicant get to the FI's website? Applicants coming from a product comparison site (e.g., BankRate) or a marketing-related email are less likely to be fraudulent than if they typed in the main URL of the FI's website. In addition, applicants coming in on a mobile device are less likely to be fraudulent as it's harder to write bots and copy/paste data from fraudulent sources. Mobile devices are used in fraudulent applications, however, so determining if a device is on a known blacklist or whitelist can provide an indication of fraud or of a valid application.

- **Examine the data elements provided.** Was a picture of an ID submitted? This is a sign of a legitimate application, as it costs fraudsters time and money to create fake IDs. In addition, it's rapidly becoming a best practice to incorporate alternative data sources (e.g., social media data, mobile network operator databases) following the Equifax breach. As one interviewee for this report put it, "We're building a 'web of authentication' that develops a score with risk factors pulled from a variety of data sources, including visible data points that verify channel access against what we already know."

- **Assess the funding source.** How was the application for a deposit product funded? An ACH transaction enables an FI to determine the age of the funding account. An account that's been in place for a while is less likely to be involved with a fraudulent application, whereas a relatively newly created prepaid account may be a red flag, as it is easier for fraudsters to create that kind of account.

- **Create cross-channel involvement.** Banks don't need to force applicants to come to the branch to prove they're who they say they are. A Facetime chat can help determine if a person looks like the person in the ID they submitted a picture of. One bank we spoke with captures voice prints of customers during phone contacts and uses those voice prints to verify applications from existing customers. It's not all high-tech, though—an online bank we interviewed said manual efforts to contact and verify applicants are required in some cases.

In addition, banks can take steps to improve today's onboarding processes, including:

- **Eliminate duplicate data entry.** *Digital Banking Report* found that many banks and credit unions still require duplicate entry of information, even when customers apply for new products from banks they already do business with. To reduce frustration, customers should never have to enter information more than once, especially when switching from one channel to another. Accomplishing this requires having "one version of the truth," which many institutions struggle to get to. Ensure information is up-to-date and in-sync across channels to reassure customers that they have anywhere-access to always-accurate data.

- **Reduce average onboarding process time.** When onboarding takes too long, consumers seek other solutions. At some banks, customers abandon up to 90% of new account applications. The root cause is legacy systems that still require manual intervention and paper-based interactions. Reduce onboarding time by: 1) Eliminating disconnected, manual processes in favor of integrated, automated processes; 2) Offering customers their choice of onboarding channels; and 3) Providing customers with process transparency.

- **Eliminate business bottlenecks.** Many banks don't have visibility into where bottlenecks exist or what's causing them. Bottlenecks typically have one or more of four causes: 1) People; 2) Process; 3) System; and/or 4) Data. Review employees' roles and responsibilities in the onboarding process for clues to identify and eliminate bottlenecks caused by people. Data issues are typically caused by legacy silos, which often produce different versions of the same document (and data).

- **Measure onboarding satisfaction.** To measure and monitor the onboarding process, banks need tools that provide information not only about past performance, current processes and how to improve them. Banks should look for: 1) Customizable dashboards that provide key performance indicators and metrics, and 2) Reporting and analytics that are tailored to facilitate faster, more informed decision-making.

CONCLUSION

Based on our research into digital identity trends, Cornerstone Advisors concludes that:

- **There is no perfect solution.** Every digital identity-related technology, approach and business model has a list of disadvantages as long as the list of advantages associated with it. To say "there is no perfect solution" may seem obvious, but many proponents of the self-sovereign model of identity write about it as if it were the end-all, be-all in identity management (although some do acknowledge weaknesses to the approach). It's not.

- **Today's investments in authentication/identity management are short-term solutions.** The speed of new developments in the identity management space (particularly regarding biometrics) means banks should take a short-term view of today's investments and anticipate new rounds of investments (i.e., replacements) in a three-year timeframe. Digital account opening, authentication and digital identity investments based on five-year (or longer) ROI timeframes are likely to be irrelevant by the third year.

- **Banks should accelerate their digital account opening and onboarding efforts.** We interviewed Brett King, author of Bank 3.0 and the CEO of neobank Moven, who said: "The first thing bank CEOs should do is develop a strategy to deliver every product without wet signature verification. They will be competing with players with the ability to do digital onboarding. It may require them to go to bat with the regulators, but they've got to do it."

- **Identity platform providers need time to evolve.** Some vendors in the digital identity space claim to already provide a "platform." Their definition of a platform doesn't jive with our ours, however. To Cornerstone, a platform is a two-sided business model that attracts providers and consumers and facilitates commerce between the parties. This means: 1) A platform isn't just a marketplace, and 2) A platform provides choice, not preset partnerships. The vendors in the digital identity space don't meet the second criteria. Just as it's taken Amazon nearly 20 years to build out its retail platform, it will take identity platform providers some time to realize the vision of a platform that enables choice and integration of vendor offerings. The good news is that FIs probably won't have to wait 20 years for this to become a reality.

- **The blockchain consortia need to spin out identity platform providers.** Consortia like R3 and CU Ledger are doing great work at developing and launching proofs of concept for blockchain applications, but becoming a full-fledged identity platform provider needs more than just technology development efforts. Building a platform requires business model development capabilities to attract other providers and users (i.e., financial institutions) to the platform. The consortia work on attracting new participants but will need to do more to build an independent identity platform.

- **No one is thinking post-device.** In all the research done for this report, we found no mention of how identity management might work in a post-device world. In other words, what if devices go away? What if technology evolves to the point where humans have identity chips embedded into them at birth? Sounds far-fetched, but few people envisioned the rapid development and adoption of the smartphone.

- **CISOs need to get more strategic.** Thirty years ago, when personal computers began to invade corporations, many CEOs recognized that their IT leaders (were they called CIOs back then?) often lacked the vision to understand how technology would impact their industries and organizations. We're in a similar situation today with bank chief information security officers. Most are technically proficient and on top of information security practices for today's world, but we fear that many lack strategic perspectives on where the digital identity world is going. Bank CEOs should challenge their CISOs to step up, or look to outside help (i.e., vendors and consultants) to get a strategic perspective.

FINAL WORD:

In all the good work going on to advance the concept of digital identity, there's a missing component that is the main impediment to change: Trust. In his book Before Babylon, Beyond Bitcoin, Dave Birch wrote:

> *"Identity is changing profoundly, and money is changing equally profoundly because of the same technological change. What will link changing identities with changing money? Trust. In a world based on trust, it will be reputation rather than regulation that will animate trust in economic exchange. The 'social graph'—the network of our social identities—will be the nexus of commerce, administration and interaction."*

Birch fails to mention whether he believes that trust exists today. Trust was also mentioned by the digital banking exec we spoke to, and we would guess he doesn't believe it exists, or why would he have brought it up? The political situation in the United States points to a lack of trust in the government among consumers to come up with a digital identity solution. Without a catalyst to improve the levels of trust, we're pessimistic that much will change at the governmental or societal level in the United States regarding digital identity, leaving bank execs to fend for themselves for the next few years.

ABOUT
CORNERSTONE ADVISORS

CORNERSTONE
ADVISORS

Cornerstone Advisors' multidisciplinary team is backed by the experience that comes from hundreds of thousands of in-the-trenches client hours. We live by the philosophy that you can't improve what you don't measure. With laser-focus measurement, financial institutions can develop more meaningful business strategies, make smarter technology decisions, and strategically re-engineer processes.

Cornerstone Advisors provides an array of Solutions offerings, including Strategy and Execution, Vendor Research, Contracts and Technology.

Cornerstone publishes GonzoBanker, our blog; the Insight Vault, a digital platform that draws on Cornerstone's exclusive research, operational benchmark data, and real-world experience; the *Cornerstone Performance Report*, a series of annual benchmarking studies; and a variety of white papers. Cornerstone hosts invitation-only roundtables for bank and credit union executives.

CONTINUE THE CONVERSATION

🌐 www.crnrstone.com
in Cornerstone Advisors
🐦 @CstoneAdvisors
☎ 480.423.2030

ENDNOTES

[1] Sovrin Trust, Sovrin: *A Protocol and Token for Self-Sovereign Identity & Decentralized Trust,* https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

[2] Unpublished quote from David Birch, author of the books *Identity is the New Money and Before Babylon, Beyond Bitcoin.* And while we include his comment to provide some humor, it may not necessarily be true anymore. A company called Onfido has developed an identity verification solution for dogs (https://hub.onfido.com/youtube-all-videos/onfidowoof-identity-verification-for-dogs).

[3] https://connect.bakerhill.com/downloadwhatsgoingoninbanking

[4] For example, see *A Survey of Biometrics Security Systems*, https://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/#sec3.4

[5] Aite Group, *Digital Authentication: New Opportunities to Enhance the Customer Journey,* September 2017

[6] American Banker, *Next-Gen Biometrics: Using the Force of Habit,* Nov. 17, 2016

[7] Tech Republic, *Biometrics and behavioral tech: The good and the bad security implications,* Aug. 11, 2015

[8] Aite Group, *Digital Authentication: New Opportunities to Enhance the Customer Journey,* Sept. 2017

[9] The FIDO Alliance is an industry consortium launched in February 2013 to address the lack of interoperability among strong authentication devices and the problems users face creating and remembering multiple usernames and passwords.

[10] Aware, *Mobile Biometric Authentication: Pros and Cons of Server and Device-Based,* January 2018

[11] PwC, *Biometrics and Privacy On Device vs On Server Matching,* May 2016

[12] https://oneworldidentity.com/identity-industry-landscape

[13] http://finiculture.com/the-identity-startup-landscape

[14] World Economic Forum, *A Blueprint for Digital Identity,* August 2016

[15] BBVA Research, *Digital Identity: the current state of affairs,* January 2018

[16] ForgeRock, *Consumer Trust, Consent and Knowledge in the Age of Digital Identity,* 2018

[17] https://techcrunch.com/2017/02/14/jaguar-launches-in-car-payments-at-shell-gas-stations/

[18] https://www.theverge.com/2018/4/18/17248282/chevrolet-shell-in-car-payment-gas

[19] UnboundID, *Identity Management for the Internet of Things,* February 2016

[20] Internet Society, *Do Blockchains Have Anything to Offer Identity,* February 2018

[21] Private interview for this report, interviewee prefers to remain anonymous

[22] TearSheet, *Credit unions are testing a blockchain-powered digital identity tool,* Nov. 2, 2017

[23] Consult Hyperion, *Digital Identity: Issue Analysis,* September 2016

[24] The General Data Protection Regulation is a regulation in European Union law on data protection and privacy for all individuals within the EU. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

[25] American Banker, *EU's new data privacy law creates headaches for U.S. banks,* Sept. 20, 2017

Have questions
about this report?

Contact:

Ron Shevlin, Director of Research
Cornerstone Advisors

rshevlin@crnrstone.com
480.424.5849