CAPCO

# JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

## SECURITY

Digital identity: The foundation for trusted transactions in financial services

KAELYN LOWMASTER | NEIL HUGHES
BENJAMIN JESSEL

# DIGITIZATION

#47
04.2018

# JOURNAL

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

# CONTENTS

## ORGANIZATION

## CURRENCY



## SECURITY

# Digital identity: The foundation for trusted transactions in financial services

**KAELYN LOWMASTER** | Principal Analyst, One World Identity
**NEIL HUGHES** | Vice President and Editor-in-Chief, One World Identity
**BENJAMIN JESSEL** | Fintech Advisor to Capco

## ABSTRACT

Navigating the digital economy has become a central component of daily life – for consumers and service providers alike. The sweeping transition from the physical to digital world has fundamentally altered the ways in which organizations transact with each other, with customers, and with regulators. This has given rise to an array of new economic possibilities, increased disintermediation, and improved user experience.

Digital technologies allow people and entities to complete high-value transactions, often without ever physically interacting. With that convenience, however, comes a key question – in a digital world, how do you know that someone is who they say they are? And beyond that initial verification, how can organizations make the critical decision to trust their counterparty? Establishing a degree of assurance that someone actually is who they are expected to be, and will do what they are expected to do is an analog problem thrown into sharp relief by the volume, velocity, and complexity of modern transactions.

The digital economy has a digital identity problem. Even though identity processes are at the core of nearly every transaction individuals and institutions undertake, most identity use cases still rely on legacy paper-based credentials. These are expensive, unsecure, and will become increasingly difficult to keep compliant as new data protection regimes emerge. For financial services institutions in particular, making effective use of digital identities is both a persistent challenge and a unique opportunity. A number of innovative models have begun to emerge to more efficiently create, verify, authenticate, and federate identity information. These distinct digital identity processes lay the foundation for enduring trust with consumers, reliable compliance with shifting regulatory regimes, and continued relevance in our brave new connected economy. Moreover, as established organizations in a highly-regulated, identity-centric industry, financial institutions are uniquely positioned to drive the development of a cross-sector identity ecosystem to address both current and future digital identity challenges.

## 1. INTRODUCTION

Since the mass adoption of the online channel in the 1990s, the financial transactions performed by individuals and companies have exploded in value, volume, and complexity. The internet has removed many of the barriers that used to exist in exchanging goods and services, as well as in moving money between individuals and companies.

The connected economy has not only transformed traditional financial and commercial transactions, but has also facilitated the rise of new transaction types. Peer-to-peer lending and credit products, mobile payments, and automated personal financial management providers, among other innovations, do not require legacy financial intermediaries. This financial technology (fintech) revolution has been a boon to consumers, who have benefited from increased access to financial services, lower transaction costs, and far less friction than they would have encountered in visiting a physical bank branch or even calling a customer service hotline.

But, even with this wave of fintech innovation, the identity problem remains. That is, how can financial institutions assert with confidence that an individual or organization they are transacting with is who they claim to be?

That enduring question is at the foundation of trusted transactions in financial services. Fintechs and legacy institutions alike are now navigating the uneasy intersection between providing a fully digital user experience and still relying on traditional physical channels to verify and authenticate counterparties. Moving forward, effective digital identity processes will become a necessary component of a connected financial services infrastructure.

In this article, we will first explore what a digital identity is and why it is central to modern financial transactions. We will then examine the particular identity-related challenges that organizations and individuals face as they look to conduct trusted financial transactions, and highlight some innovations in the digital identity space that aim to solve these challenges. Finally, we will look ahead at the unique opportunities financial institutions may have to drive cross-sector adoption of digital identity ecosystems and facilitate future development in the space.

## 2. THE NEED FOR DIGITAL IDENTITY

Currently more than 60% of American consumers bank primarily online,[1] with estimates indicating that over 70% of internet users in the U.S. will use digital banking by the end of 2018.[2] In a world where the majority of financial transactions are moving to a digital channel, digital identity will have enormous consequences. Digital identity is a multi-dimensional challenge that underpins not only financial transactions, but also access to a wide array of online services.

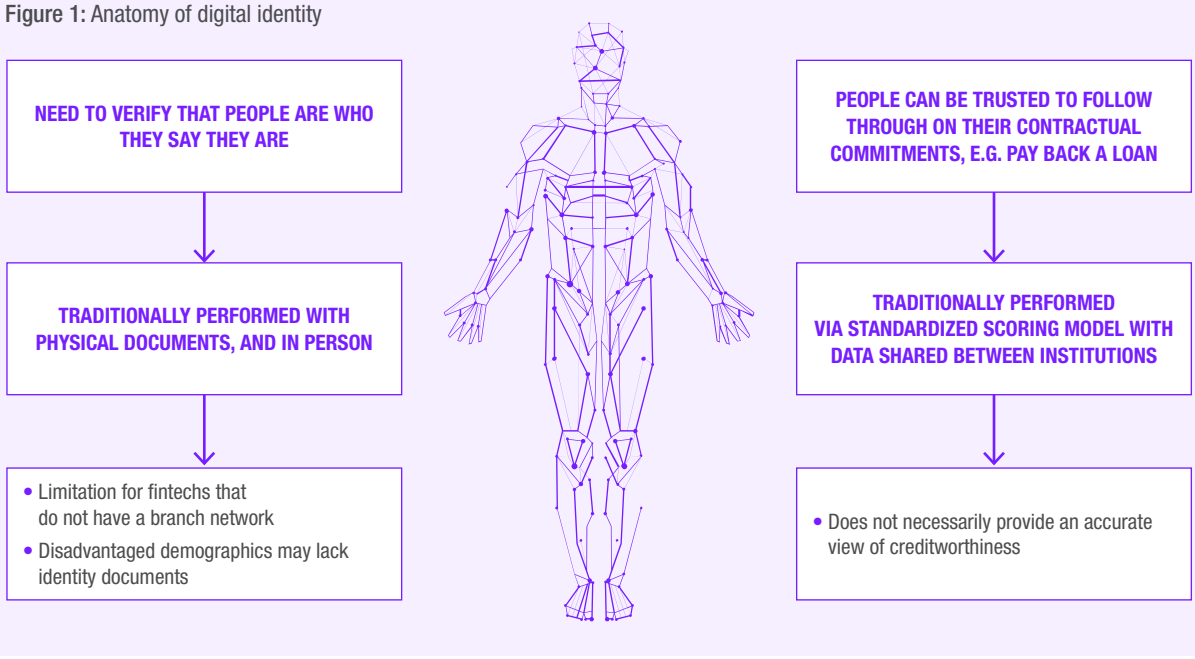
The digital identity challenge in financial transactions is far-reaching, but we will examine it here in the context of two broad, interrelated issues – verification and trust.

First, the ability to confirm that a counterparty really is who they claim to be is a primary component of transaction legitimacy. From a regulatory perspective, compliance with existing "know your customer" (KYC) and "anti-money laundering" (AML) statutes requires accurate identity verification. Even in today's digital economy, however, a consumer looking to open a checking account or apply for a mortgage often must provide physical documents in order to verify their identity and create a record with their financial institution. These legacy verification procedures are often expensive for service providers, inconvenient for users, and time-consuming for all involved. This is particularly true for markets in which traditional identity documents and credentials are hard to come by. Verification is also, in many cases, repetitive and localized to a particular service. That is, a customer must often undergo repeated checks of the same information, often requiring in-person appearances with physical documents to access different services. By the same token, financial services providers are left with the burden of secure storage or destruction of "personally identifiable information" (PII), presenting additional potential security and compliance issues.

This enduring reliance on physical identity verification also presents an especially targeted challenge for emerging fintechs. These organizations typically do not have a physical branch network and are aiming to deliver a direct-to-consumer online- or mobile-only experience, highlighting the urgent need for effective identity verification in digital channels.

[1] Statista, 2018, "Share of American population primarily using digital banking from 2014 to 2016," http://bit.ly/2BYkfXu; HM Treasury's 2015 Budget Report, March 18, 53 (Section 1.204), 98 (Section 2.272)
[2] Statista, 2018, "Penetration of digital banking among internet users in the United States from 2013 to 2018," http://bit.ly/2oGrjBY

**Figure 1:** Anatomy of digital identity




Second, financial institutions rely upon effective identity processes to establish counterparty trust. Confirming trustworthiness establishes a level of confidence that a customer or partner organization will actually carry out their obligations as mutually agreed in a given transaction. When counterparty trust is low or difficult to confirm, some form of recourse (either legal or through holding collateral) can provide protection in the case that one of the parties does not follow through on their obligations. Either way, an accurate evaluation of counterparty trust is contingent upon an accurate understanding of counterparty identity.

Traditional financial institutions have tended to approach trust assessment using a very limited set of identity data.[3] Evaluations of creditworthiness typically rely on a decades-old credit scoring model (like FICO) to make determinations on whether to enter into a transaction that incurs a level of risk on the bank's behalf (Figure 1). Legacy scoring models are blunt instruments, however, that exclude millions of people worldwide, especially younger consumers or those in developing markets, who may not have the credit history or physical identity documents to be "scorable" by traditional financial institutions.

Moreover, the centrality of these traditional financial institutions is being eroded in the digital economy. Increasingly, counterparties in a digital financial transaction are not banks, but rather another individual or entity. This is especially apparent in the sharing economy, where individuals are starting to monetize the excess capacity of their assets, including property (as with Airbnb or HomeAway), ride sharing (like Uber or Lyft), or even peer-to-peer lending networks (like LendingClub or Prosper). The success of these platforms is rooted firmly in trust established by a firm confidence in counterparty identity. In order for an Uber transaction to take place successfully, for example, a rider must have confidence that the person picking them up is, in fact, the correct driver, that the driver is properly licensed and insured, that the rider has entered valid payment information, and that neither the driver nor Uber itself will improperly exploit the wide array of identifying information the rider has shared (including payment information, mobile number, or location data). Each of these is a distinct identity use case that relies entirely upon the efficient, secure, and entirely digital processing of identities.

[3] For additional information on identity data and trust assessment, see OWI, 2017, "Bad credit? No credit? Big identity problem: the definitive primer on identity data in credit scoring," One World Identity, July 25, http://bit.ly/2CNV8Wf

## 3. ANATOMY OF A DIGITAL IDENTITY

Digital identities, then, are at the core of nearly every interaction between individuals, companies, and even devices, as the "internet of things" (IoT) continues to expand. Users rely on a variety of identities depending on the transaction at hand. The digital identity used for a Facebook profile, for example, relies on substantially different attributes, review procedures, and access protocols than the digital identity a bank uses to establish a new customer account. In order to understand how financial institutions can best apply emerging technologies to this complex problem set, it is worth dissecting the anatomy of digital identity processes in more detail.

The problem of digital identity involves multiple distinct processes that broadly encompass what attributes can be used to identify an individual, how to prove them over time, when to share them, and what a person can do with them. Given that digital identity is a broad topic, we need to define it with an additional level of granularity via the basic framework shown below, which provides five core digital identity use cases, along with the challenges and priorities inherent in each.

| CREATION | VERIFICATION | AUTHENTIFICATION | AUTHORIZATION | FEDERATION |
|---|---|---|---|---|
| An authoritative process demarcating a particular attribute or set of attributes of an individual, entity, or object (e.g. contract, website, property, bank account), such that the attribute(s) can be used in future transactions to prove existence and uniqueness | The process of confirming at least one attribute of an individual or entity, either through self-attestation or third-party confirmation | The process of determining that one is transacting with the same entity iteratively over time | The process of determining what rights or privileges an individual or entity should be granted | The process of conveying an individual's or entity's verification, authentication, or authorization information to another party |
| Who are you? | How do we prove who you are? | How do we know it's still you? | What do you get once we know it's you? | How can we tell other people it's you? |

### 3.1 Creation

Identity creation, the process of establishing trusted credentials that can be used in future transactions, is the first step in the digital identity lifecycle. Creation is an authoritative process demarcating a particular attribute or set of attributes of an individual, entity, or thing, such that the attributes can be used in future transactions to demonstrate the existence and uniqueness of that individual, entity, or thing.

For most individuals in the world, identity creation takes place in the form of government birth registration. For example, in the U.S., birth registration catalogues several attributes – name, gender, date and location of birth, and citizenship – that are fundamental to identity-related transactions throughout a person's lifetime. Governments may also mandate other identity creation processes, such as the creation of a national identification number to access benefits or pay taxes, or a motor vehicle licensing authority that can create attributes such as the type of driver's license or license restrictions. Often these same hard-copy government credentials, issued as part of basic civil registration, are required to create new records or apply for accounts with financial institutions.

Agreeing on an schema of attributes to collect for organization-specific identity creation processes can be challenging, especially when standardizing transactions internally across different departments or regions. For example, the due diligence requirements of a financial institution in Thailand are very different from those in the U.S. Similarly, it is very common for international banks with Swiss entities to interpret the attributes of an owner of a bank account in a very different way than would a U.S. division.

Identity creation involves collecting information on a person or entity, across a set of agreed-upon attributes. This specific process raises questions surrounding what organization should be collecting the data, and

the means by which personal identity information should be kept up to date and relevant. In the case of financial services, organizations such as KYC.com have established clearing houses of identity data to enable customers to conduct more efficient KYC checks.

However, identity creation still presents a looming problem in many parts of the world. It is estimated that 1.1 billion people globally currently lack an officially recognized identity, and around 375 million adults in developing markets are unable to access financial services due to lack of required identity documentation.[4] In the absence of reliable government infrastructure to register people born or companies formed within a country's borders, often there is a void for other mechanisms of identity creation.

## 3.2 Verification

The second step of the identity lifecycle, verification, has been referenced in the previous section as especially problematic for financial institutions. Identity verification refers to the process of confirming at least one attribute of an individual or entity, either through self-attestation or third-party confirmation. Sometimes referred to as "identity proofing," verification looks to prove that trusted credentials or attributes are connected to the intended individual.

Identity verification is frequently discussed in the context of financial services: KYC and AML protocols rely on effective verification procedures. Financial institutions must rely on a combination of user-provided information and third-party attestations (the government may attest to a citizen's social security number, a utility company to a customer's address) to prove that prospective customers truly are who they say they are. Only with a verified identity can financial institutions initiate trusted transactions.

## 3.3 Authentication

Identity authentication, the third component of the identity lifecycle, is the process of determining that an organization is transacting with the same individual or entity iteratively over time.

The classic example of authentication in the digital age is the ubiquitous username and password. When a customer logs into their bank account, their financial institution needs to know that the person accessing the account is, in fact, the account's owner. Logging in with a username and password is one means of indicating to the institution that it is dealing with the same person in each transaction. Note that authentication does not necessarily require verification – that is, for standalone authentication procedures the particular identity attributes of the entity being authenticated are not being examined, as long as the authenticator can confirm that the entity is identical across transactions.

There are multiple additional methods for conducting digital authentication procedures, some of which can involve multiple factors to enhance security and reliability. For example, combining something the user knows (like a password), with something the user has (a device or credential), something the user is (a biometric marker like a fingerprint or iris scan), or something the user does (behavioral biometric analysis).

To that end, security and user experience are the twin primary concerns with most authentication procedures, and the two are often inversely related in legacy systems. As people access more disparate services online, it is increasingly convenient for them to reuse passwords across service providers. Various studies report that between 70-90% of consumers reuse passwords. This erodes security for individuals whose personal information is more likely to be compromised, and leads to enormous costs for institutions in the form of theft or compliance fines.

More secure technologies for digital identity authentication exist in various stages of development (multi-factor authentication, biometrics, and behavioral analytics, to name a few), but can be less convenient for users and difficult for entrenched institutions to adopt. Advanced biological and behavioral biometrics have also tended to provoke privacy concerns in some markets. Improving both security and user experience simultaneously is the primary driver for much of the technological innovation for this use case.

## 3.4 Authorization

Authorization is the process of determining what users can and cannot do based on their digital identity. It typically takes a combination of verification and authentication events to grant a user permission to perform certain actions. For example, after logging into their Netflix account, a customer will be granted access to streaming services based on their status as a paying member. However, if that user travels outside the U.S., they may not be authorized to view certain content based on a change in their location, a core identity

[4] ID4D, 2017, "Making everyone count," Identification for Development, World Bank, http://bit.ly/2FGgYxY


attribute in this transaction. From a service provider's prospective, effective authorization procedures involve robust internal process flows built on a foundation of accurate verification and authentication processes. A trend in authorization has been to move from role-based (a defined set of static permissions) to attribute-based (a more dynamic set of permissions).

Authorization fundamentally requires flexibility, as both roles and attributes change frequently and users authenticate (or fail to authenticate) into systems on a regular basis. Failure to accurately monitor key identity attributes could lead to illegitimate access of sensitive information or costly services. At the same time, however, it is an untenable burden for companies, in terms of both cost and security, to undergo continuous identity verification for all customers in order to ensure roles and attributes have remained constant for authorization purposes.

## 3.5 Federation

Identity federation is often the last step of a given digital identity lifecycle. Federation is the process of linking a digital identity or specific identity attributes across multiple distinct systems, or even across different service providers.

Establishing methods to execute federated identities has become increasingly attractive as the ratio of online to physical interactions increases. The most visible manifestation of identity federation are "single-sign on" (SSO) configurations by which a user can access multiple service providers through a single authentication process. Depending on the nature of the transaction, a service provider can federate an entity's verified, authenticated, or authorized identity – any of those functions can be shared. Identity federation is one approach toward reducing the burden of duplicative procedures outlined above.

In the world of access to social platforms, Facebook, in particular, has become a common federated identity service provider. Through the platform's 0Auth 2.0 capability, developers of digital services can connect their platforms to Facebook, with Facebook validating their login and then providing an agreed set of personal data to that application. In this particular case, maintaining that information is largely the user's responsibility. In other applications of federated identities, however, the consequences of stale, incorrect, or improperly shared data can have severe consequences.

Securing personally identifiable data is a challenge within one siloed service provider, and that problem only multiplies as identities are shared across institutions. With multiple interconnected accounts, the difficulty of achieving illegitimate access decreases while the incentive for doing so rises dramatically. Data ownership and consent also becomes an issue with federation — users are often not aware of how their identity data is used across accounts, and lose control of who can access their data and for what purposes.

Underpinning these five distinct identity building blocks are industry-, sector-, or jurisdiction-specific sets of identity standards. Standards concern an agreement between organizations and entities that are involved in a transaction with regards to what attributes of a customer are sufficient to create a trusted digital identity, and how that digital identity can then be verified, authenticated, and federated. An increasing number of government institutions and private sector consortium groups are advocating for open identity standards to bolster security, privacy, and user experience across identity use cases. However, identity standards can be very different depending on what is being transacted or what service is being accessed, and many are still evolving as technologies develop.

## 4. IDENTITY CHALLENGES FOR FINANCIAL INSTITUTIONS

Despite the unprecedented technological development and innovation in the financial services sector, financial institutions still face a number of considerable challenges in integrating digital identities into their services across these five identity lifecycle stages. Digital identity issues in the financial services space fall into a few major categories:

- **Administrative costs,** including manual verification, legacy record storage, and customer service costs.
- **Service delivery challenges,** including inability to tailor service offerings, inaccurate pricing, and customer exclusion.
- **Risk and compliance challenges,** including escalating KYC and AML costs as well as navigating new regulatory regimes like the E.U.'s General Data Protection Regulation (GDPR) and revised Payment Services Directive (PSD2).
- **Theft and fraud,** including escalating new account fraud, account takeover, and synthetic identity fraud.

Given the roadblocks currently in place, progress in this area has been slow, though there are opportunities to address each of these challenges through effective identity ecosystem development. Consider that under the current systems, customers must re-share the same identity information every time they want to do something as basic as opening a bank account or applying for a credit card. As improvements in digital identity become more universal, these additional steps should become a thing of the past, as banks gain access to decentralized and verifiable forms of identity that allow them to accept each other's approvals.

### 4.1 Administrative costs

Incomplete, ineffective, or outdated identity systems represent a significant cost to financial services providers and customers alike. When onboarding a customer, initial identity creation, verification, authentication, and authorization processes require individuals or entities to present physical documents or conduct in-person visits. As discussed above, manual verification of physical credentials represents a substantial investment of time and resources. The average cost of an in-person transaction is around U.S.$4.25, while mobile transactions reduce that figure to only U.S.$0.10.[5] Where fully digital identity authentications can take place using voice confirmation or biometric scanning technology, for example, transaction costs can be greatly reduced.

In the U.K., for example, 25% of financial services applications are abandoned by customers due to friction created by KYC.[6] Steps such as login or payment verification present challenges across a range of industries, but they are particularly problematic in banking. For example, roughly 30% of calls to bank call centers are requests for account access.[7] It's estimated that each of these calls can cost a company around U.S.$25 – a princely sum for basic customer service, all over something as simple as a forgotten password. In this way, a lack of digital identity represents a direct cost inefficiency to service providers and consumers alike.

### 4.2 Service delivery challenges

Financial services organizations can also gain advantages by analyzing customer identity data they have already collected and are not yet using. This is because data about customers has been traditionally housed in the individual, transactional systems outlined above, and are typically not well integrated across organizational divisions. This is known as a data silo, where an abundance of information about a customer is available, but is operationally unusable. Without the ability to intelligently interpret the data already collected, banks are unable to connect the dots and compose an integrated view of the customer.

[5] Fiserv, 2016, "Mobile banking adoption: where is the revenue for financial institutions?" https://fisv.co/2oEqLME

[6] Meola, A., 2016, "E-Commerce retailers are losing their customers because of this one critical mistake," BusinessInsider, March 16, http://read.bi/1puwynf

[7] Accenture, 2013, "The future of identity in banking," https://accntu.re/1S3FaHb

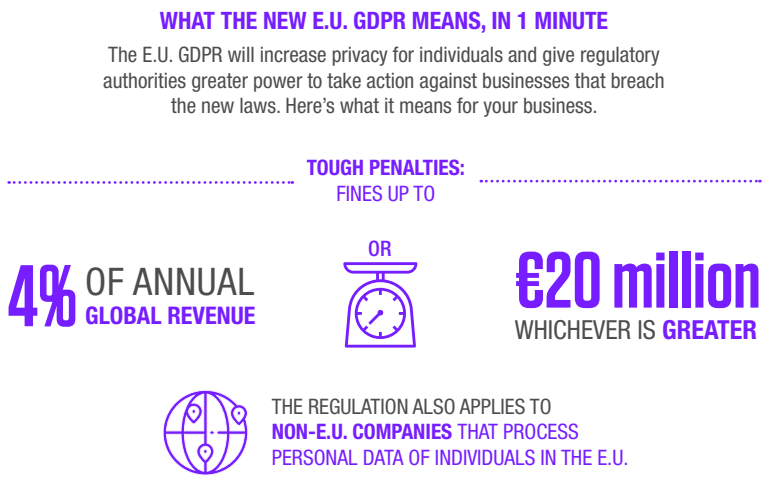
This poor management of customer identity can lead to a wide array of missed opportunities in service delivery. Consumer pricing, for example, is key in the financial sector. Here, banks could build targeted propositions to customers with pricing that reflects that customer's relationship with the bank. Institutions could also draw from rich transaction history data, which offers key insights into their buying habits. Banks, however, are not usually in a position to do this. For example, a bank would not want to price a personal loan independently of a mortgage – instead, they are likely to provide a competitive price that reflects the potential share of the consumer's available funds. The result is a fragmented situation, where each product line of a bank interacts with a customer as if it is the customer's first time doing business with that bank. From the customer's perspective, this is an impersonal and inefficient way of doing business. This issue was recently highlighted by Nomis, which found that banks can have over 300,000 pricing points across as many as 300 retail locations. And customers have taken notice – a Capgemini survey found that just 37% of customers believe banks understand their needs and preferences adequately.[8]

More broadly, lack of digitization throughout the consumer lifecycle, including reliance on physical identity creation and verification channels, excludes millions of potential financial services consumers. In the financial services sector alone, digitization could bring an additional 1.6 billion customers from developing markets into the formal economy, creating U.S.$4.2 trillion in new deposits and U.S.$2.1 trillion in new lines of credit.[9]

## 4.3 Risk and compliance challenges

The increased complexity of finance in the digital age has also led to an array of new issues related to compliance and risk, many of which have their roots in identity processes. Consider cross-border payments, where user verification can present a significant challenge. Correspondent banks in western financial hubs, such as New York or London, may be asked to handle payments from counterparties with accounts from countries where identity standards policies are less strict. It would be impractical for a bank to perform due diligence on each and every counterparty and transaction. As a result, institutions instead rely on algorithms intended to track payment flows and flag suspicious behavior. Unfortunately, in practice, these methods are not particularly effective, determining the probability of fraudulent activity without certainty. It is

**Figure 2:** E.U.'s GDPR




Source: IT Governance

estimated that financial institutions spent more than U.S.$8 billion on AML efforts in 2017, and it's expected that those investments will grow by 9% in 2018.[10]

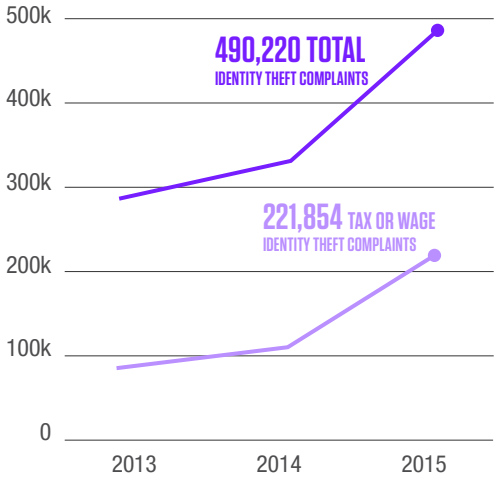
These identity challenges may become even more acute in 2018 and beyond. There are larger challenges on the horizon, including upcoming regulations that govern how data about customers can be gathered, used, and stored. For example, the General Data Protection Regulation (GDPR) (Figure 2) will place significant restrictions on the lifecycle of consumer data used by financial institutions, resulting in stiff penalties for noncompliance – up to 4% of global revenue or €20 million, whichever is greater. GDPR will also require that data collected about customers be commensurate with the product that the data is collected for. As a result, financial institutions will not be able to indiscriminately build up datasets on customers in anticipation that this information could potentially be used at a later point in time. GDPR also includes a "right to be forgotten" clause that will require financial institutions to delete all data concerning a customer when requested. Since many large banks have data trapped in silos, the lack of a centralized repository of customer information will only compound problems for these institutions. The global fortune 500 will spend an

[8] CapGemini, 2017, "Big data alchemy: how can banks maximize the value of their customer data?" http://bit.ly/2oKmZ4K

[9] Manyika, J., S. Lund, M. Singer, O. White, and C. Berry, 2016, "How digital finance could boost growth in emerging economies," McKinsey & Co., http://bit.ly/2z9Tpcm

[10] PwC, 2018, "Pulling fraud out of the shadows: the biggest competitor you didn't know you had," https://pwc.to/2sKL1xF

**Figure 3:** Identity theft




Source: Krebs on Security

estimated U.S.$8 billion to become GDPR compliant, and digitizing the identity management lifecycle will be a priority to stay in line with this new data protection regime.[11]

GDPR is not the only transformational regulatory regime reshaping the financial services sector, however. The Revised Payment Services Directive (PSD2) in the E.U. is aimed at modernizing European payment infrastructure and spurring innovation in payments and financial services. Its key provisions include a move toward "open banking," wherein existing financial services institutions must make consumer account information available to third parties (including new fintech players). PSD2 will lower barriers to entry for non-traditional financial players. This means that traditional financial institutions will no longer be able to rely on data access as an exclusive competitive advantage, and will be forced to innovate based on trusted consumer experience.

## 4.4 Theft and fraud

Identity management efforts with limited resources also inevitably lead to bad actors slipping through the cracks. Financial institutions are well aware that the vectors for theft and fraud evolve as quickly as the technological tools to contain them.[12] 15.4 million Americans were the victims of identity fraud in 2016, with losses totaling U.S.$16 billion.[13] Worldwide identity theft costs are estimated to be at least U.S.$221 billion.[14] Currently, an estimated 1 in 9 digital account creation attempts are fraudulent, as are around 1 in 20 digital login attempts.[15] Traditional identity processes are simply insufficient to contain digital threats.

The problem of synthetic identity fraud is a particularly urgent symptom of the existing identity problem. Fraud committed by consumers using synthetic identities – that is, exploiting weak identity creation and verification processes by combining a series of legitimate attributes to form a new, fictional identity – is growing. Up to 20 percent of defaulted credit card debt may already be the result of synthetic identity fraud, and the technique already costs businesses more than U.S.$6 billion annually.[16] For financial institutions, the problem is exacerbated by the lack of integrated customer records as discussed above.

## 5. IDENTITY AND TRUST IN FINANCIAL INSTITUTIONS

Beyond these direct revenue, compliance, and fraud considerations driving financial institutions to implement digital identity processes, identity is also a foundational component of trust and safety. The ability to execute trusted, secure transactions is a core mandate for legacy financial institutions looking to maintain market share as the landscape of alternative digital and mobile financial service options continues to expand. Connected customers, fatigued by 2017's unprecedented personal data breaches and able to select from a growing array of innovative financial products, make their choices based on trust. For traditional financial institutions, this means that trust is a core product offering – as quantifiable and impactful as any credit vehicle.

Broadly, trust and safety[17] refers to the full set of business values and practices that increase participation in and engagement with a digital ecosystem by reducing the risk of harm, fraud, or other criminal behavior toward an individual or organization and its reputation. Trust also requires that institutions have proper recourse mechanisms in place for redressing the damage of adverse events when they occur. By establishing a

[11] IAPP and EY, 2017, "2017 privacy governance report," http://bit.ly/2GVjgsl
[12] For more information on common identity-based vectors for theft and fraud see OWI, 2018, "Personal data management fundamentals," One World Identity, January 30, http://bit.ly/2s7i0Qq
[13] Pascual, A., K. Marchini, and S. Miller, 2017, "2017 identity fraud: securing the connected life," Javelin Strategy, http://bit.ly/2mYmaDi
[14] Carbajo, M., 2013, "How to prevent and detect business identity theft," U.S. Small Business Administration, January 9, http://bit.ly/1E16rsR
[15] ThreatMatrix, 2017, "Cybercrime report 2017: year in review," http://bit.ly/2oGlynN
[16] Auriemma Consulting Group, 2017, "Synthetic identity fraud cost banks $6 Billion in 2016," BusinessInsider, August 1, http://read.bi/2F90S27
[17] OWI, 2017, "Commitment issues: trust & safety through the digital fog," One World Identity, October 30, http://bit.ly/2GRx4E9

basic threshold of trust, a stakeholder will choose to participate in a particular digital ecosystem. Maintaining a sense of safety ensures nothing goes wrong when participating in that ecosystem.

Effective digital identity processes underpin the trust-building financial institutions must prioritize. They need to do so with two distinct constituencies: customers and regulators.

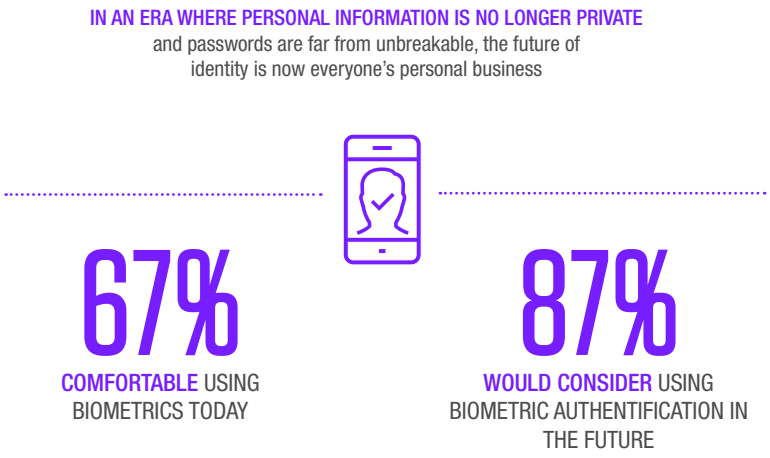
With customers, effective digital identity processes have the potential to minimize friction in user experience and enhance data security, both key pillars of trust and safety.[18] For example, new research indicates that customers more likely to trust financial institutions that use advanced technology like biometrics for identity verification and authentication.[19] In fact, over 40% of consumers would refuse to use a digital financial service that is not secured by some sort of biometric authentication.[20] Lack of user familiarity has often been cited as a primary obstacle in the adoption of new authentication technologies, but that is increasingly untrue. Customers now carry advanced fingerprint and facial recognition technology in their pockets, and are now increasingly demanding digital identity verification, authentication, and authorization as part of financial transactions. Simple passwords and traditional knowledge-based authentication mechanisms are, rightly, no longer as trusted.

Building trust with regulators is a related, but substantially more complex process. 2018 may prove to be a turning point for the regulation of personal data in markets around the world, and financial institutions must be proactive in building their identity data stewardship infrastructure to avoid crippling fines or sanctions under GDPR, PSD2, the Chinese Cybersecurity Law, or any of the other emerging data governance regimes under which they may fall. Each of these statutes requires financial institutions to have thorough knowledge of the personal identity data they collect, the business processes for which it is used, and the manner in which it is stored. Robust digital identity processes throughout the consumer lifecycle – from onboarding through the termination of the business relationship (which, under GDPR, may require the destruction of all personal data) – are a requirement for modern compliance.

When that trust is lost, financial institutions face potentially disastrous financial and reputational costs. On the consumer side, customers have exhibited decreasing trust in traditional banking institutions year over year.[21] Nearly 90% of customers say they will abandon a service provider that does not manage their personal identity data responsibly.[22] Overall, the average cost of reputation damage of lost trust due to identity data compromise ranges from U.S.$184 to U.S.$332 million.[23] In the case of Wells Fargo, for example, illegitimate use of personal data directly impacting around 3% of customers ended up costing the company an estimated U.S.$99 billion in deposits, and almost a third of existing customers reported looking elsewhere for banking services.[24] Quite simply, lack of trust costs banks customers, and digital identities are necessary for trust.

The good news for financial institutions, however, is that trust-building provides a ripe opportunity for innovation and differentiation. Currently only about a third of customers perceive significant differentiation between financial services providers based on product offerings alone.[25] For that reason, improving user experience and security through reliable and frictionless digital identity

**Figure 4:** The future of identity




Source: IBM Biometrics

[18] OWI, 2018, "Five pillars of trust and safety," One World Identity, January 5, http://bit.ly/2oFp3ut
[19] Sposito, S., 2018, "Two-factor authentication: even Google struggles to enroll users," Javelin Strategy, February 5, http://bit.ly/2FaPH98
[20] Security, 2017, "Consumers trust biometrics for mobile banking and payments," May 6, http://bit.ly/2HU98RO
[21] EY, 2017, "The relevance challenge: what retail banks must do to remain in the game," https://go.ey.com/2ihm5sl
[22] Kawamoto, D., 2017, "Consumers don't trust businesses can protect their data," DarkReading, http://ubm.io/2zcit6k
[23] Ponemon Institute, 2011, "Reputation impact of a data breach: U.S. study of executives & managers," http://bit.ly/2CQ8OzO
[24] White, G. B., 2017, "The toll of Wells Fargo's account scandal," The Atlantic, April 19, http://theatln.tc/2Fa9eXf

creation, verification, and authentication procedures can itself be a differentiator in the increasingly crowded market for digital financial services. Effective digital identity processes, and the trust they engender with customers, are a competitive advantage that financial institutions should explore.

## 6. FINANCIAL INSTITUTIONS AND THE FUTURE OF DIGITAL IDENTITY

Financial institutions are fundamentally identity-centric institutions. For trusted transactions to take place in the digital economy, institutions must invest in constructing effective digital identity infrastructure throughout the customer identity lifecycle. While this will require significant attention to mitigating the identity challenges outlined above, it also means that financial institutions are uniquely positioned to support the development of digital identity ecosystems across sectors.

Traditionally, the financial institutions have been a key component of an identity architecture from the perspective of enabling merchants and customers to confirm that they are who they say they are. For example, in credit card networks, both merchants and customers are validated by banks.

However, financial services landscape is increasingly moving toward a less tightly-bound ecosystem. For instance, the frequency of cross-border transactions is increasing, involving customers and client organizations who are members of non-domestic banks with different verification standards. Peer-to-peer lending organizations and non-depository payment providers are proliferating, such that there may be no traditional banks involved in a financial transaction. Gaps in the existing digital identity structure are becoming a significant constraint, particularly as fintech organizations continue to enter and disrupt the market.

This is where financial institutions have a potential role to play. These institutions are trusted with processing large amounts of persona data, and have been performing an identity broker role in some form for some significant time. Financial institutions, therefore, have the opportunity to offer identity verification, authentication, and federation services to organizations both within the financial services sector, and even in cross-sector use cases.

Recent research has already highlighted the extensive potential for financial institutions to facilitate identity services in both public and private sector interactions.[26] Indeed, in some markets, new nationwide identity infrastructure layers are being constructed driven primarily by financial institution participation.

The U.K.'s GOV.UK Verify system, for example, allows users to access public sector services online after their identity is verified by a private company of the user's choice, like Barclay's or Experian. In Canada, SecureKey Concierge follows a similar model with several financial institutions serving as identity providers for citizens to access dozens government services. Sweden's BankID platform facilitates identity services for 2 billion transactions per year.[27] BankID has recently integrated next generation identity verification and authentication mechanisms based on behavioral biometrics to minimize reliance on passwords. Six of the country's largest banks also cooperatively launched a common mobile payment app, Swish, in 2012, building on BankID's functionality.

Exporting identity services has already proven to be a successful endeavor for traditional financial institutions in these markets. Institutional liability and trust risks remain, however, as this business model continues to mature. If Bank A relies on Bank B's attestation of a customer's identity, for example, and that initial attestation is later determined to have been insufficiently thorough, Bank A could feasibly have recourse to pursue damages for any fraud committed in some jurisdictions. At a time when financial institutions are receiving unprecedented fines for lax customer due diligence, this could be an area in which some organizations have a low appetite for risk.

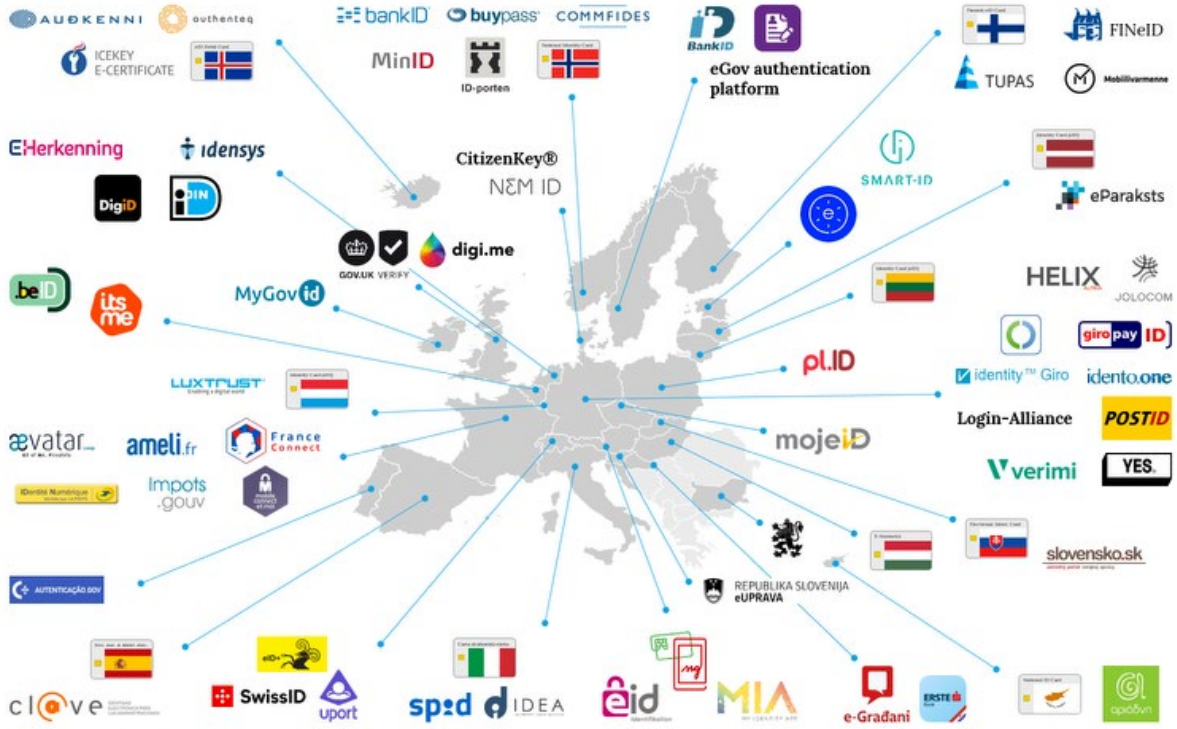
Nevertheless, as legacy banks struggle to maintain relevance and market share in an increasingly decentralized financial services sector, digital identity, and the consumer trust it engenders, could itself be a profitable service offering in the connected economy.

[25] EY, 2017, "The relevance challenge: what retail banks must do to remain in the game," https://go.ey.com/2ihm5sl

[26] World Economic Forum, 2016, "A blueprint for digital identity: the role of financial institutions in building digital identity," http://bit.ly/2aOblg1

[27] Metzger, M., 2016, "ISSE 2016: The four models of digital identity," SC Media, November 23, http://bit.ly/2HVKAr0

Figure 5: Key identity initiatives within Europe

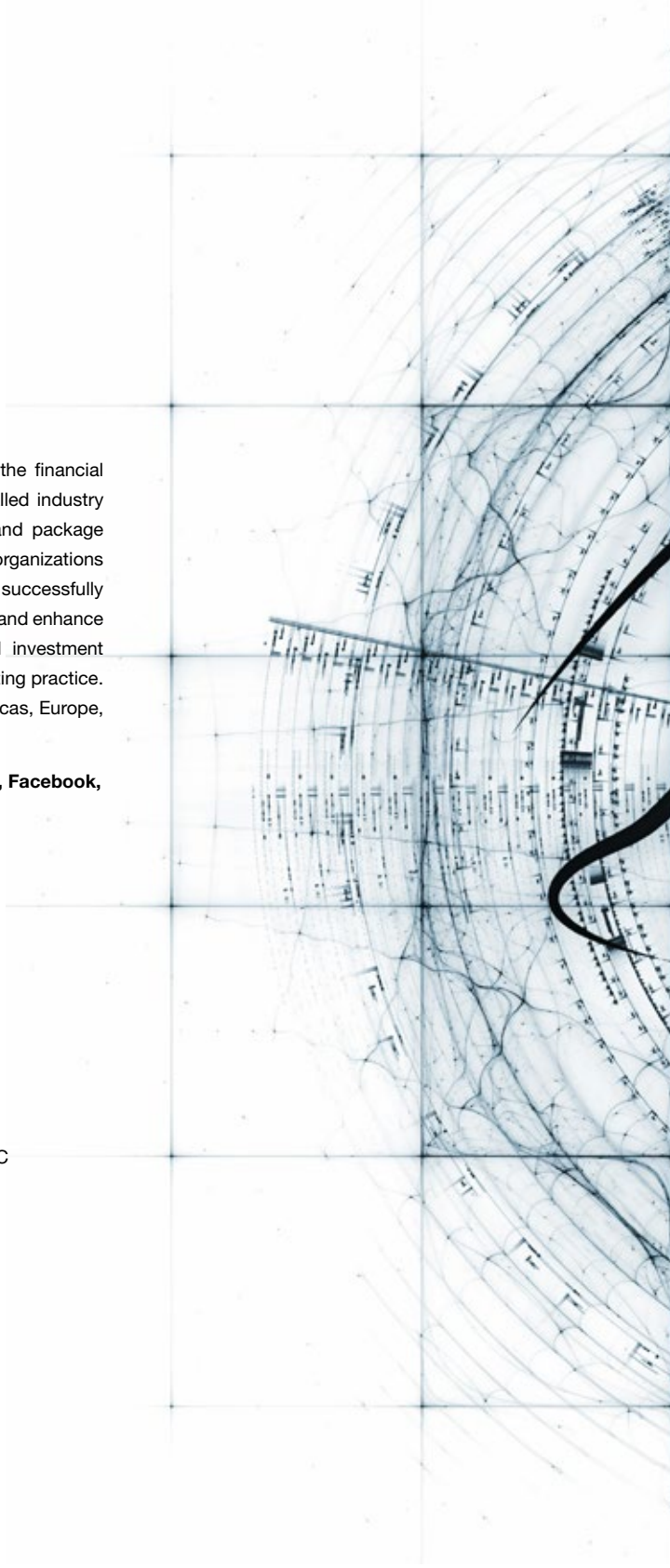



Source: asquared

## 7. CONCLUSIONS AND A LOOK AHEAD

Identity – of customers, client organizations, and partner entities – is at the heart of the financial services industry. Without effective identity processes, clients and regulators lose trust, financial institutions lose money, and legacy institutions lose out to the alternative financial services players emerging as part of the fintech wave. But, within the identity challenge lies an immense opportunity for financial institutions to build the infrastructure for future cross-sector digital identity ecosystems. A few core lessons will help financial institutions adapt to the reality of the connected economy and lead the evolution of digital identity:

- **Legacy, paper-based identity processes are expensive and unreliable.** Traditional identity creation, verification, and authentication procedures in particular are costing financial institutions not just money, but also time, trust, and competitive edge. Innovative identity solutions, including advanced authentication mechanisms like biometrics and behavioral analytics, improved internal data stewardship, and enhanced digital and mobile service offerings, can significantly reduce administrative costs, bolster security, and improve customer engagement.
- **Effective digital identity systems are necessary for institutional survival.** In today's digital economy, trust in traditional financial institutions is falling, and customers are less likely to perceive differentiation between banks based on product offerings alone. A more educated generation of financial consumers will choose to interact with financial institutions they trust. Robust digital identity processes build trust and safety with users and regulators by enhancing user experience and security. Both will be required for banks to stay relevant.
- **With new regulatory regimes, data access is no longer a competitive advantage, but trusted identity services can be.** 2018 will be a year of fundamental shifts in the regulatory landscape. Barriers to entry for innovative fintechs are falling, but the standards for collecting, sharing, and storing identity data are more stringent than ever. Banks are no longer the sole custodians of customers' economic destiny. Establishing trust through frictionless and secure digital identity processes will be key for customer retention.
- **Financial institutions are uniquely positioned to underpin digital identity ecosystem.** As developing identity ecosystems like those in the U.K., Canada, and the Nordic countries have demonstrated, financial institutions are uniquely positioned to drive the development of digital identity ecosystems that extend across the public and private sectors. Demand for effective digital identities is growing in nearly every consumer-facing industry, and financial institutions can play a key role in providing the identity services as the foundation of trusted transactions for years to come.



## ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com, or follow us on Twitter, Facebook, YouTube, LinkedIn and Xing.**

## WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM



CAPCO