IDENTITY VERIFICATION IN BANKING

HOW BANKS ARE USING NEW AUTHENTICATION METHODS TO BOOST CONVERSIONS AND KEEP THEIR CUSTOMERS LOYAL

February 2018

Maria Terekhova | Research Analyst

BI INTELLIGENCE

KEY POINTS

- **The strict verification standards that banks are subject to have led them to create onboarding and login processes that are arduous for clients.** Additionally, they face a paradox in that the verification methods they use to remain compliant can actually end up compromising customers' personal data. As a result, banks are grappling with diminished customer satisfaction and loyalty, as well as security breaches that lead to compensation payouts and legal costs.

- **This problem has existed for some time, but a convergence of factors is now pushing banks to attempt to remedy it.** These include a more complex regulatory environment and increasing competition from digitally savvy startups. Additionally, consumers' expectations for the user experience are being set higher by companies outside of finance, such as Google, Amazon, and Facebook, where speedy onboarding and intuitive service is a given.

- **For banks, the trick is to streamline verification for clients without compromising accuracy, and several emerging technologies promise to deliver that result.** These include biometrics, optical character recognition (OCR) technology, cryptography, secure video links, and blockchain and distributed ledger technology (DLT). Such technologies are increasingly being used in live environments to replace legacy methods, and more mainstream mobile devices, which many people use to conduct their banking, are now being made to support them.

- **However, technology is only one piece of the puzzle when it comes to producing viable new identity verification methods.** Choice of collaborators, including the industries and countries they operate in, greatly influences the usability of any new solution. As such, banks are partnering not only with tech-savvy fintechs, but also with cross-industry consortia and governments to bring new verification solutions to market.

- **The long-term opportunity such innovation presents goes far beyond streamlining processes.** Banks are already experts in vouching for people's identities, and because they're held to such tight security standards, their testimonies are universally trusted. If banks figure out how to successfully digitize customer identification, this could help them not only boost revenue and cut costs, but secure a place for themselves in a modern economy, where online identities will be key to carrying out transactions.

Download the charts and associated data in Excel »

INTRODUCTION

The way incumbent banks onboard and verify the identities of their clients online is inconvenient and insecure, resulting in diminished customer satisfaction and loyalty, and security breaches leading to compensation payouts and legal costs. It's a lose-lose situation, as consumers become disgruntled and banks lose business.

The problem stems from the very strict verification standards and high noncompliance fines that banks are subject to, given the high capital volumes they manage daily. This has led them to prioritize stringency over user experience in verification. At the same time, verification is unavoidable and ubiquitous: Banks are mandated to subject clients to strict identity checks when users want to do things like open accounts, make transfers, or access their accounts abroad, creating multiple consumer pain points. They also face a paradox in that the verification methods they use to remain compliant can actually end up compromising customers' personal data.

However, banks can no longer afford to prioritize stringent verification at the cost of user experience. Onboarding and verification standards are increasingly being set by more tech-savvy, consumer-centric players both within and outside their industries, such as fintechs and e-retailers. If banks wish to retain customer loyalty, they must begin innovating in this area. The trick is to streamline verification for clients without compromising accuracy. If banks manage to do this, the result will be happier and more loyal customers; higher client retention and revenue; and less spending on redundant checks, compensation for breaches, and regulatory fines.

The long-term opportunity such innovation presents is even broader. Banks are already experts in vouching for people's identities, and because they're held to such tight verification standards, their testimonies are universally trusted. As such, if banks figure out how to successfully digitize customer identification, this could help them not only boost revenue and cut costs, but secure a place for themselves in an emerging platform economy, where online identities will be key to carrying out transactions. This report will look at the biggest pitfalls in current verification methods that need to be fixed, the technologies available to help banks do so, and what they stand to gain from revamping this complex process.

WHAT IS IDENTITY VERIFICATION, AND WHY IS IT BECOMING A PROBLEM FOR BANKS?

Identity verification is the process by which service providers, including financial institutions (FIs), verify that a client (either an individual or a business) is the party it claims to be. Verification takes place in two stages: during onboarding, and on a transactional basis when a client wants to log into a session. Customers will typically have to confirm they are who they say they are to access online statements, authorize money transfers, and access their accounts when abroad. Essentially, this involves matching an identifier a customer submits at login to corresponding information linked to that identifier on an FI's database.

Banks are held to very strict anti-money laundering (AML) and know-your-customer (KYC) standards to ensure that they don't facilitate illicit financial activity, and failure to thoroughly comply with these regulations incurs steep fines or even prosecution. As a result, banks require customers to verify themselves when accessing any service they provide, and often multiple times in a single session.

These verification procedures may keep banks compliant, but they result in customer friction. At login, most verification systems rely on passwords, or what Brett McDowell, executive director of the FIDO Alliance, a strong authentication standards group, calls "shared secrets." This approach is problematic because customers are asked to create a password with each of their service providers, which is a hassle and results in the stress of having to remember multiple secret codes. Additionally, as banking shifts from online to mobile, typing passwords, especially complex ones with special symbols, on a small screen and keyboard is uncomfortable, causing typos, delays, and even blocked access if enough mistaken attempts are made.

Impact Of Inefficient KYC And Sanctions Remediation Processes On UK FIs' Business

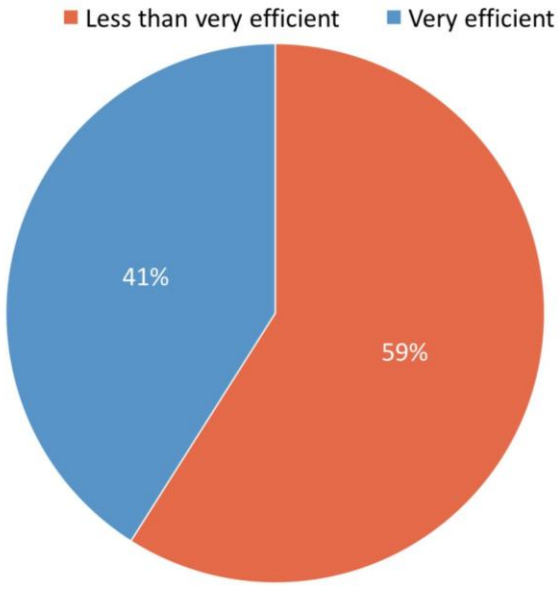
% indicating a rating of moderate to significant negative impact

Source: LexisNexis, n=151, 2017

BI INTELLIGENCE

Efficiency Of KYC And Sanctions Remediation Processes At UK FIs

Self-reported

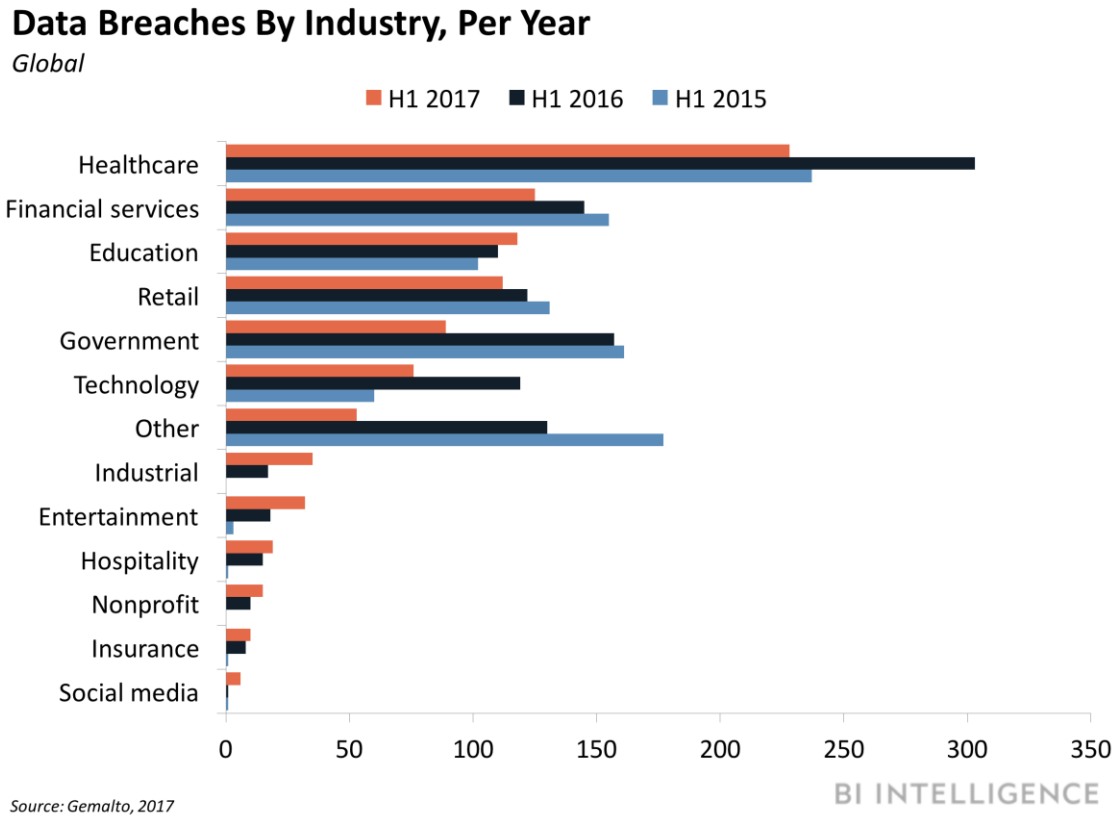


Source: LexisNexis, n=151, 2017

BI INTELLIGENCE

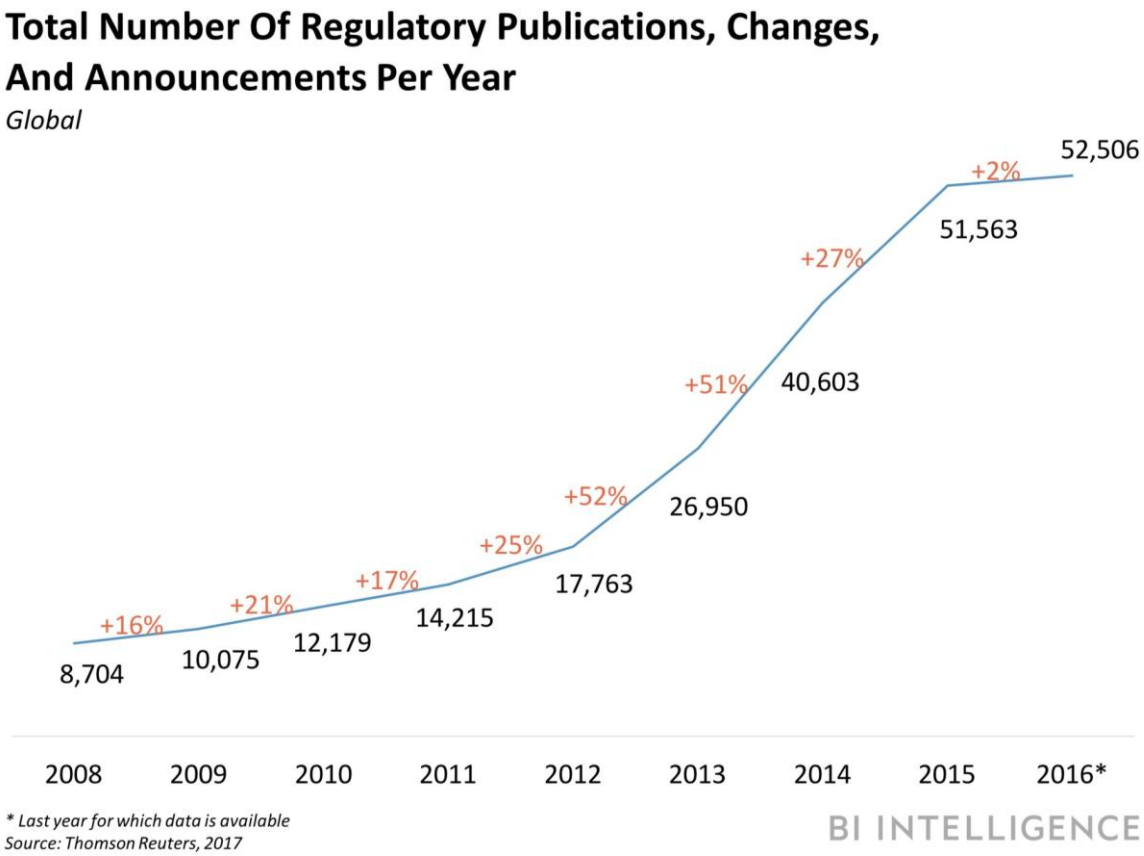
Moreover, this approach can result in customers' data becoming compromised. Because remembering shared secrets across institutions is so frustrating, customers often re-use passwords, make them exceedingly simple so they're easier to remember, or even write them all down somewhere that others may see them — all of which compromise security. If a password that's been used across portals is breached in one place, it becomes easy for a cybercriminal to automate an attack by randomly testing the password at other institutions where the individual is a client, for example. Making matters worse, most banks store all clients' personal information in a single, central database, so if just one account is breached, the whole database can be compromised in one go.

These vulnerabilities are actively and increasingly being exploited, as hacks at major institutions including US credit bureau Equifax, Tesco Bank, and Lloyds Bank, to name just a few, have illustrated in recent years. This should be especially galling for banks, as an institution can spend as much as $500 million annually to make the security of its verification solutions robust. However, reliance on a password model undermines these efforts, meaning that such spending sometimes proves futile.

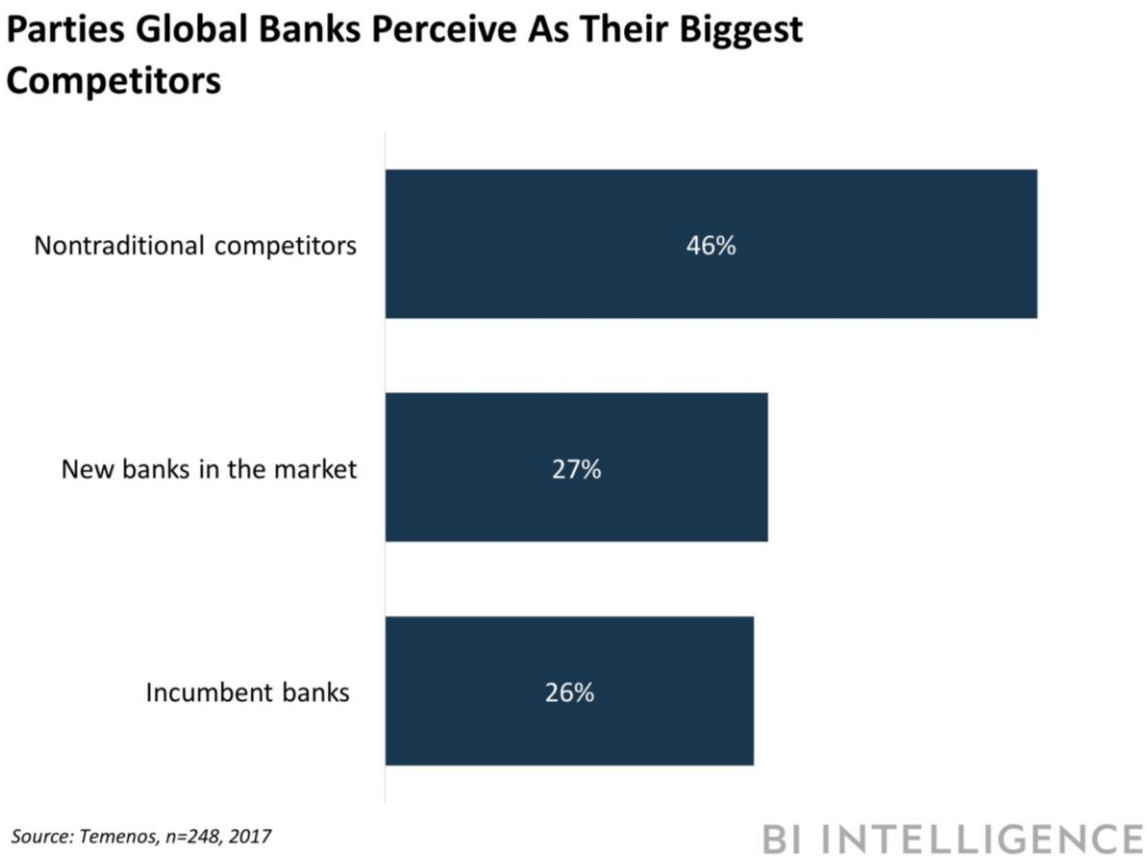


The issues posed by this approach have been apparent for a long time. However, banks are now facing a new problem: The economy they operate in is rapidly digitizing, and virtually all transactions are moving online in every industry. Correspondingly, as customers seek to access all their banking services online, verification procedures must also be adapted to a digital environment. The need to update these measures now is being driven by several factors:

A more complex regulatory environment. Banks have always been held to very strict data security standards by regulators, making their compliance burdens enormous, but several impending laws will further exacerbate this problem. Besides existing KYC and AML regulations, banks in the EU and beyond will now have to comply with the General Data Protection Regulation (GDPR), due to be implemented in May 2018. This law will impose massive fines on banks for improperly using, storing, and protecting customer data, and for failing to publicly disclose security breaches in a matter of hours. GDPR also coincides with the introduction of Europe's PSD2 and the UK's Open Banking laws, which mandate banks share their customer data (with users' permission) and systems with third parties, raising more data usage and security concerns. As identity verification procedures require customers to submit often sensitive personal and financial information, any misuse or breach of such information would have a particularly heavy impact on the banks storing and handling it.



Increasing competition. Competition is intensifying from fintechs without their own banking licenses, such as Tide, Pockit, and Monese in the UK. These players' strengths lie in the convenient app and user interfaces they provide that allow them to offer a variety of products without a full license, so it makes little difference to their users which institutions hold their money. Their agile IT infrastructure allows them to greatly streamline the onboarding process: Opening a Tide account, for example, takes minutes and requires only a driver's license or passport. By contrast, it can take weeks to set up accounts at a legacy bank. For challenger banks, the mean score for convenience of onboarding and verification was 9.2/10, compared with 7/10 for incumbents, according to a recent study by PaID Strategies. These ranking were based on metrics including duration of and number of steps involved in onboarding, and days before an account could be used.

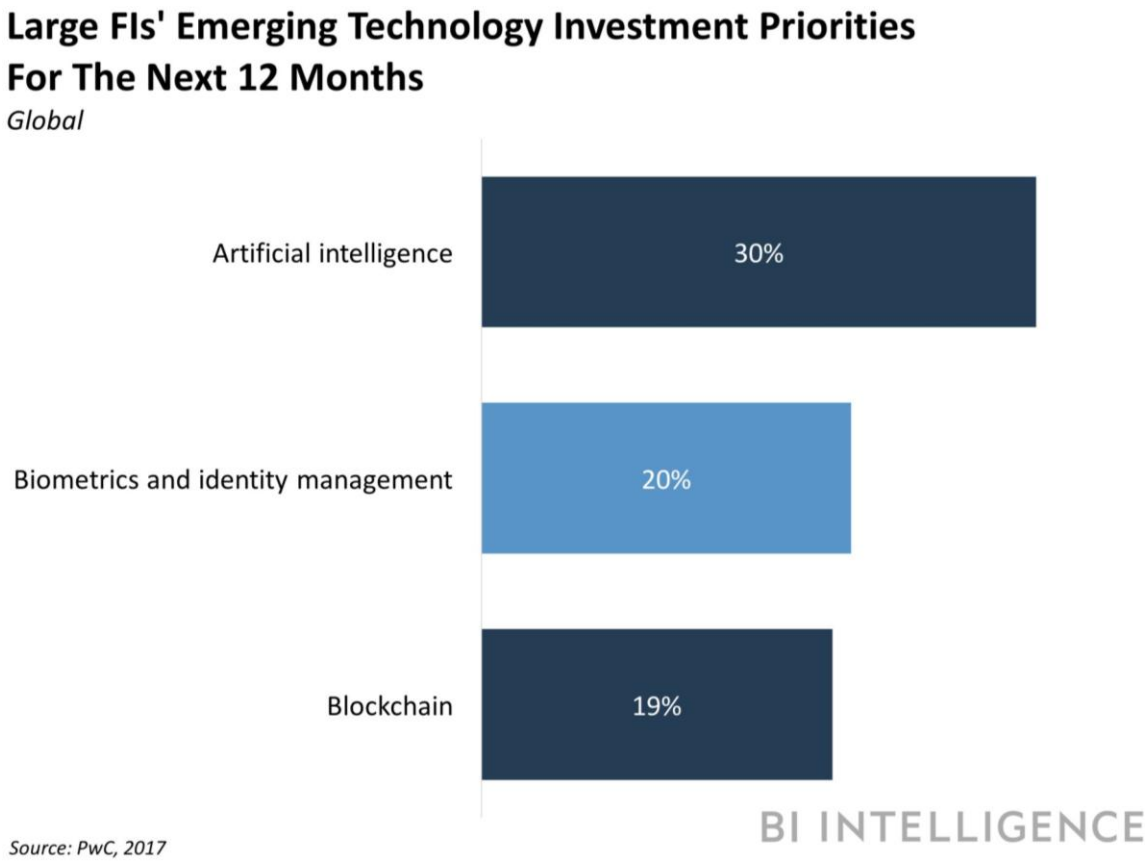


Consumers' expectations of user experience are also being set higher by companies outside of finance, such as Google, Amazon, and Facebook, where speedy onboarding and intuitive service is a given. This is upping the stakes even more for banks to improve their authentication processes, especially as many incumbents are convinced these players will soon push aggressively into financial services. Moreover, Facebook bought identity verification software company Confirm in January 2018, indicating that such firms are actively thinking about innovation in this area specifically.

THE NEXT GENERATION OF IDENTITY VERIFICATION SOLUTIONS

The emergence of new and nascent technologies, including biometrics and secure video links, is giving banks a path forward to revamp their identity verification procedures. These technologies are increasingly being used in live environments to replace legacy methods, and more mainstream mobile devices, which many people use to conduct their banking, are now being made to support them. New ways of using more established technologies are also being found to help banks in this area.

Below, we look at the technologies being leveraged in the next generation of identity verification solutions, and how banks are applying them in real-world environments:



Biometrics

Biometric technology enables a bank to identify and verify an individual customer based on a data point or set that's unique to the physical individual, such as a voice pattern, iris, fingerprint, vein pattern, or facial features. This data is used to compile a biometric profile that the bank stores in a database or other secure repository, and then uses as a template against which to verify the user when they swipe a fingerprint or look into their screen. Numerous banks are already rolling out biometric verification to customers, including TSB, HSBC, most retail banks in the UK, MayBank in Malaysia, and major Japanese card network JCB. Biometrics offer high convenience, as all the user has to do is touch or look at their phone to log into a service. It also boosts security for the bank, as users don't have to write down passwords that can be lost.

Among those pioneering the use of biometrics for identity verification is Spanish bank BBVA, which colaunched Veridas, a new tech company specializing in digital identity tools, in collaboration with biometrics and nanotechnology startup Das-Nano in November 2017. Veridas will focus on developing customer verification and authentication software, which will vouch for the identity of BBVA clients online using facial, voice, fingerprint, image, and document recognition technology. BBVA says such solutions will make online logins and transactions more secure and convenient for consumers.

In the digital ID space, it's important for a single or very select number of solutions to gain widespread adoption with as many players as possible, as the point of a single online digital ID is primarily convenience. BBVA is already distributing its banking services via third parties through its application programming interface (API) marketplace, so it could use this existing supplier network, with their customer bases, to disseminate the digital ID solutions that emerge from Veridas. This would likely prove an effective way for BBVA to ensure its digital ID achieves the necessary network effect, making the bank the leading provider in this space.

Optical Character Recognition (OCR)

OCR technology extracts data from physical documents, enabling an institution to easily search and edit the information collected by running it through software, such as AI algorithms. Until recently, OCR was used largely to automate the archiving and searching of documents, but it's now being put to use in identity verification. OCR can efficiently conduct and automate background checks, which is especially useful in simplifying the verification of business clients.

ID verification fintech Trulioo launched a business client verification solution in October 2017 that uses OCR, and can automatically authenticate a business' credentials on a bank's behalf by searching hundreds of government databases. It also allows FIs to request additional information like business registration documents, and check a business against criminal watchlists. The solution is capable of validating vital credentials from 250 million companies in real time, accessing over 180 public databases, including government records, and verifying businesses from over 84 countries, according to Trulioo.

Although many new identity verification solutions have tended to focus on verifying individuals, verifying a business is often trickier than a single person, as the entity in question is larger and interacts with more parties, meaning more factors have to be taken into account. As such, business-focused solutions may actually be in higher demand among banks, especially larger players that cater heavily to corporate clients. This demand is likely to intensify further under more stringent KYC regulations, including the 4MLD in the EU.

Cryptography

Cryptography is a method of data transmission by which information is encrypted to make it unreadable in transit. It's used to ensure that only the intended recipient of the data can decipher and read it. There are many forms of cryptography, but the one getting the most attention on the verification front is asymmetric key cryptography. A “key” is a randomly generated unique number; in this process, two nonidentical keys are paired, meaning that one can only be activated, and the information it protects unlocked, by its pair number. One of the numbers can be shared with any party, a “public” key, while the other is private. Either number can be used to scramble a message, and the opposite one used to decipher it. This ensures the information relayed between a bank and a specific customer cannot be intercepted.

Private keys are often stored in users’ mobile devices, and are unlocked with biometric identifiers, commonly by swiping a fingerprint on a sensor. This absolves banks from relying on a vulnerable central database. Moreover, that the key usually must be unlocked with a fingerprint makes it very hard to access the information it protects. This was illustrated by the US government’s inability to break into a terrorist’s iPhone in 2016, following Apple’s refusal to divulge either of the necessary keys. It's also a powerful example of the greater control asymmetric key cryptography gives individuals over their own data.

One of the most advanced solutions using this technology currently comes from Covault, a US-based verification fintech backed by BBVA's New Digital Businesses unit. Covault launched a mobile app in December 2017 designed to make storing, sharing, and verifying online identities more streamlined for banks and customers. It combines key encryption and biometric signatures that have to be entered on a user's device, making it almost impossible for information to be accessed without the user's authorization.

Meanwhile, in September 2017, ING's Belgian arm started allowing its customers to access its services using itsme, a digital identity app developed by banks Belfius, BNP Paribas Fortis, KBC/CBC, and ING, in collaboration with telecommunications companies Orange, Proximus, and Telenet. ING customers in Belgium can now use the app to log into their bank accounts and approve banking transactions. itsme's developers say that several insurers and retailers are also planning to incorporate the app in the near future. The mobile app aims to remove the need for consumers to use multiple passwords, usernames, tokens, and card readers to navigate between different service portals on the internet. Instead, they can simply download itsme onto their phones, and use a single cryptographically generated code when they need to log into an internet service that requires ID verification, within the network of participating businesses.

Digital identity solutions like itsme are proliferating, and as more enter the market, it will be harder for consumers to use a single solution across their services, mitigating the convenience the technology is meant to provide. As such, the leading solution in this space will be the one that can onboard the most institutions across multiple industries quickly, so cross-industry verification projects are a logical strategy. But collaborating with companies not bound by banks' KYC and AML laws chances bringing up compliance and security risks for banks.

Secure Video Link

Establishing a secure video connection between a computer at a bank’s office and one in a user’s home allows bank staff to visually confirm a user’s identity against a scanned document via an in-person interview. Typically, a secure video link is introduced as a substitute for onboarding, rather than subsequent verification, as it makes most sense to deploy this tech to replace a process that usually requires an in-person meeting.

Big banks are already deploying this method: BBVA launched Online Onboarding in November 2016, which allows consumers to open a BBVA account in a matter of minutes via their mobile device and use their account immediately. A user first has to download BBVA's banking app. Then, they must upload a photo ID and take a selfie that the bank can verify using facial-recognition technology. In the final step, a BBVA employee confirms the new customer's identity via a video call; staff are available 24/7 to do this.

This is a relatively simple tweak, but spares new customers from having to go to a branch. Moreover, it helps banks retain a personal element when onboarding a client, helping to build stronger customer relationships.

Blockchain And Distributed Ledger Technology (DLT)

Blockchain and DLT are essentially shared ledgers that promise greater transparency and immutability in transactions by requiring records to be confirmed by multiple users with access to the data. Banks are now looking at implementing these technologies in identity verification procedures; 79% of banks said blockchain technology can reduce time and risk by making it easier to perform KYC and AML checks in their consumer lending business, according to one IBM study.

Benefits of blockchain and DL technologies in identity verification include giving consumers better control over their data, and helping FIs avoid noncompliance with GDPR strictures on data storage and usage. However, major obstacles stand in the way of blockchain- and DLT-based solutions moving beyond the proof of concept (POC) stage, including questions on how to intervene in a supposedly immutable ledger if a mistake is somehow made. Many FIs are also struggling to find the tech talent necessary to fully understand the nascent technology and bring solutions based on it to market, making these technologies perhaps the least viable replacement in practical terms for current verification methods, for now.

Interestingly, however, blockchain and DL technologies seem to be attracting the most attention from FIs looking to revamp their identity verification methods. A wide range of approaches to apply the technology to this process have already emerged, suggesting that bringing solutions based on these technologies to fruition is very difficult, and that the gains appear big enough for banks to explore many alternatives to make them a reality. Here are a few examples:

- **Trust-Hive.** Leading FIs including AG Insurance, BNP Paribas Fortis, Euroclear, KBC, and SWIFT are working with Belgian fintech center B-Hive to develop a blockchain-based digital identity platform called Trust-Hive. The platform, they say, will give customers better control over how their identity data is handled and stored by organizations, in compliance with GDPR. Trust-Hive will also save FIs money on redundant authentication procedures by storing a customer's credentials in a central portal, which can be accessed by FIs with the consumer's consent. Drawing on the talent and ideas of a fintech network could help ensure that Trust-Hive is fully optimized for a consumer-centric economy, while outsourcing at least some of the solution's development should help incumbents reduce outlays on the project. If the prototype is successful, the parties plan to roll out Trust-Hive across Europe in 2018.

- **Red Lyra.** Spanish banks Sabadell, Santander, BBVA, Bankia, BME, and Caja Rural, along with numerous domestic players from other industries, cofounded Red Lyra in June 2017, a project that aims to get companies using DLT and smart contracts to develop new digital services focused on digital identity. The goal is to develop solutions that will help companies digitally validate the identities of individual customers and counterparties to streamline customer onboarding, as well as issue and authorize digital signatures within a legal framework. A national initiative may fare better for digital identity than an international one, as identity verification is still a very national affair, with different jurisdictions taking different approaches to validating individuals' authentication. This will likely be exacerbated by the current geopolitical environment, as well as widening regulatory gaps as GDPR lands in the EU.

- **Singapore's KYC blockchain.** Major APAC banks OCBC, HSBC, and Mitsubishi UFJ Financial Group (MUFG), together with Singapore's Infocomm Media Development Authority, successfully built a prototype for a KYC system based on blockchain technology in October 2017. This new solution will store identity information on a distributed network, which can then be securely accessed by FIs. This will help make applying for a bank account more efficient and cost-effective for banks, and convenient for customers, as clients won't need to come to the branch. The consortium tested the KYC blockchain between February and May 2017, and concluded that it's scalable and secure. Collaboration with government and public sector entities is emerging as one of the most effective ways for banks to develop viable new verification solutions, as it reduces the risk of building noncompliant alternatives, and can help produce a single, standardized verification solution that can then be disseminated across multiple institutions, reducing the risk of a plethora of new, noncompatible solutions proliferating. Similar efforts are underway in Sweden and India.

THE NEXT FRONTIER OF DIGITAL IDENTITY VERIFICATION

As more identity verification methods emerge from incumbent banks, nonbank companies, and fintechs, it raises the chance that too many competing solutions will arise, creating new pain points for consumers by making it harder for them to use a single solution across all their services. This saturation point already seems to be on the horizon, as illustrated by a patent clash between two German startups over similar video link technologies in 2017.

As such, we'll soon start to see consolidation and standardization across identity verification projects. Toward this end, the FIDO Alliance established its European Working Group in November 2017, which aims to help companies across the EU modernize their authentication solutions in compliance with PSD2 SCA by using open industry standards and emerging best practices. FIDO's McDowell says that "confusing users is asking for trouble," but is confident that the industry "will land on a best practice that does not depend on the user being a security expert." Covault CEO Louie Gasparini adds that all banks would benefit from a common standard, and it would be attractive for them to converge to one, even a peer's solution, as there's a lot of overlap in design across current prototypes. A common standard would ultimately result in cost savings and efficiency for all adopters.

It therefore seems probable that innovation around identity verification will converge on collaboration between private companies (including banks) and public bodies, such as government departments, or at least on cross-industry working groups, to maximize the network effect of any prototypes. The end goal of any such initiative, arguably, should be to move away from verification and refocus on providing consumers with a single digital identity that can be used across all digital services.

This could present a major opportunity for banks in an emerging platform economy, as UBS notes in a white paper. That's because, with their expertise in regulatory compliance and their unparalleled high security standards, banks could become critical providers of consumers' digital identities, thus securing them a central role in a new digital landscape. Juan Losa, a senior executive at Veridas, concurs, saying that a "cross-industry digital identity is feasible," and that banks' verification solutions can add value anywhere from retailers to restaurants.

THE BOTTOM LINE

- The strict verification standards that banks are subject to have led them to create onboarding and login processes that are arduous for clients. Additionally, they face a paradox in that the verification methods they use to remain compliant can actually end up compromising customers' personal data.

- This problem has existed for some time, but a convergence of factors is now pushing banks to attempt to remedy it. These include a more complex regulatory environment and increasing competition from digitally savvy startups.

- For banks, the trick is to streamline verification for clients without compromising accuracy, and several emerging technologies promise to deliver that result. These include biometrics, OCR technology, cryptography, secure video links, and blockchain and DLT.

- Choice of collaborators, including the industries and countries they operate in, greatly influences the usability of any new solution. As such, banks are partnering not only with tech-savvy fintechs, but also with cross-industry consortia and governments to bring new verification solutions to market.

- If banks figure out how to successfully digitize customer identification, this could help them not only boost revenue and cut costs, but secure a place for themselves in a modern economy, where online identities will be key to carrying out transactions.

BI INTELLIGENCE

BI Intelligence, Business Insider's premium research service, provides in-depth insight, data, and analysis of everything digital. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key areas of tech: mobile, e-commerce, digital media, payments, the Internet of Things, transportation and logistics and more.

If your organization would like to learn more about our research, including a license to republish our charts, please contact: intelligence@businessinsider.com