SAMSUNG SDS AMERICA

WHITE PAPER

The Identity Verification Challenge: Solving the KYC Problem First

Contents

The Identity Verification Challenge: Solving the KYC Problem First

Spurred to strengthen data security measures and improve ease-of-use for customers, many banks have replaced passwords with digital identity solutions including biometric authentication. While a more convenient and secure approach, biometric enrollment without an upfront identity verification process puts customers' banking apps at risk when their phones are stolen. Fortunately, by marrying "Know Your Customer" (KYC) identification practices and biometric enrollment, financial firms can eliminate this growing problem. And with new identity verification tools, organizations can bring higher accuracy, speed, and efficiency to their KYC process.

From banking to payments to wealth management, almost every type of financial activity is being transformed by mobile, cloud, and other new technologies. For the financial services industry, this shift is helping to reignite growth and rebuild customer trust. In fact, the Consumers and Mobile Financial Services report shows the number of mobile phone owners using a mobile banking app has doubled over the last five years, reaching 43% in 2015.[1] In response, some banking giants, including Bank of America, have closed brick-and-mortar locations to focus more on mobile, online, and ATM services.[2]

But with new technologies come new challenges, particularly regarding data security and identity verification.

The Evolution of Authentication Methods

Until recently, consumers could access all their website accounts and mobile apps with a username and password. Over time this form of one-factor authentication has proven less and less secure as people choose trivial passwords that are easily guessed, leave their passwords on sticky notes, or set their web browser to store their passwords. Moreover, numerous people use the same username and password across different online accounts, making it easy for a hacker who steals a customer's credentials from one site to immediately gain access to many other sites they use. In fact, the latest Verizon Data Breach Investigations Report found that 81% of hacking-related breaches used either stolen and/or weak passwords.[3]

Realizing the pitfalls of one-factor authentication, many financial institutions have moved to two-factor authentication (2FA)—the digital equivalent of a combination lock with a changing code. A popular 2FA method is the use of a one-time password (OTP) token in the form of a passcode or pin being delivered via email, phone call, or SMS message. These tokens are usually valid for 60 seconds (+/- 10 seconds).

Over time, OTP tokens have proved vulnerable to man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks, and create problems and frustration for customers due to delivery delays, network coverage issues, and security risks when no identity verification method is applied. In fact, recent guidance from the National Institute of Standards and Technology (SP800-63B Digital Identity Guidelines) recommends removal of OTP via email and instead advises for higher-assurance authentication, central to the FIDO approach.

These issues have spurred the next evolution in security: use of biometric authentication. Different from passwords, biometrics relies on personalized features, such as fingerprint, face, iris, and voice—which are difficult to duplicate—to authenticate users.

Biometrics Replaces Passwords with Stronger Security and Convenience

Since the early 1980s, biometric systems of identification and authentication using voice, fingerprint, or iris scan were used for guarding mainframe access or restricting physical entry to high-security areas. Today, biometric technology is being used by almost every industry as a convenient, reliable, and secure method to safeguard websites, mobile apps, and corporate databases.

According to Gartner, by 2020 new biometric methods will displace passwords and fingerprints for access to end-point devices across 80% of the market.[4] Not surprising given that more than 500 biometric smartphone models have been introduced since Q1 2013.[5] This includes smartphones incorporating fingerprint, iris, and eye vein biometrics from market leaders such as Samsung, Apple, Lenovo, and ZTE. According to Acuity Market Research, 1 billion biometric smartphones are in use today, representing 40% of the global installed base of smartphones.[6]

Among the financial services industry, growth in biometric use is being led by banks acknowledging that traditional passwords are either too cumbersome or no longer secure. Some of the nation's largest banks, including Bank of America, JPMorgan Chase, TSB, Barclays, and Wells Fargo, are increasingly using fingerprints, facial scans, and other types of biometrics to safeguard accounts.[7][8] For example, customers are being asked to provide a biometric identifier and answer a security question to perform certain financial transactions, like transferring funds or making a purchase.

By 2020 new biometric methods will displace passwords and fingerprints for access to end-point devices across 80% of the market.

Source: Gartner Research[9]

Undoubtedly biometric authentication is a more convenient and secure approach for customers, but without an upfront identity verification process prior to biometric enrollment the method fails to safeguard against fraud.

With the current process, establishing biometric identification on a banking app requires little more than logging in and scanning a fingerprint, voice, or iris. Whether that fingerprint, voice, or iris belongs to the rightful account owner is never actually verified. Herein lies the problem.

Fortunately, financial service organizations can take steps to better align existing processes and utilize new identity verification tools to reduce fraud.

The Need to Combine KYC Requirements and Biometrics

In an effort to safeguard our financial systems, governments have pushed increasingly stringent regulations on financial service firms. One such requirement, the "Know Your Customer" (KYC) regulation, forces financial institutions and regulated companies to perform greater due diligence to identify, document, and authenticate the customer prior to any engagement.[10]

Nowhere is KYC's impact more prominent than during the customer onboarding process.

Most major banks allow customers to submit an application for an account or a loan online. However, in order to remain KYC-compliant, many banks require customers to provide a copy of their driver's license, birth certificate, or passport to prove their physical identity. This may involve scanning an ID and sending it directly to a bank or financial firm for verification, or visiting a branch to present an ID in person.

Despite these more rigorous identity verification efforts, last year an estimated 15.4 million consumers were impacted by identity theft, up from 13.1 million the year before.[11] [12] Theft involving cell phone account takeovers alone—which helps criminals gain access to financial accounts—doubled in the past year.[13]

The key to meeting KYC regulations and protecting customers' identities is to merge the two processes. This means onboarding customers should concurrently involve physical or digital ID verification and biometric enrollment.

Major banking institutions have recognized this problem and are taking steps to improve their KYC efforts and safeguard customers' accounts. What are they doing? This paper should give banks some guidance or best-practice insights.

New Tools Ensure KYC Process Is Accurate, Fast, and Efficient

While consumers want stronger identity verification and data protection measures, they balk at a process that is inconvenient, takes too long, or is just plain painful. In today's instant-access era, waiting even a day to finalize an account represents an eternity for customers. Unfortunately, a 2016 Thomson Reuters global survey reveals that banks are taking as long as 48 days to onboard a new customer, and spending in excess of US$60 million per annum on KYC and client onboarding.[14]

"Advances in security and verification will enable all aspects of sales, service, and delivery to be conducted online."

PWC Report - Retail Banking 2020: Evolution or Revolution?[15]

The result: Consumers are opting out. In fact, one company's analysis of online abandonment rates found the financial service industry has the second highest, with an average of 79% of transactions being abandoned (the travel industry ranked number one).[16] Considering how much money banks and other financial institutions spend to attract new customers and grow their share of wallet among existing customers, the number is alarming.

Fortunately, new regulatory technologies (regtech) from leading providers such as Samsung SDS offer new ways to verify IDs (e.g., replace paper-based with digital processes using e-forms and e-signatures) to authenticate users, with biometrics, and onboard customers completely online. These new services allow banks, investment companies, and financial firms to reshape traditional practices, such as opening a new account or applying for a line of credit, to be KYC-compliant and conducted completely online.

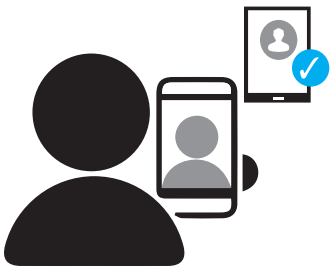
These services include:

ID Verification Services

Many financial organizations rely on someone at a branch or use an offshore site to visually verify an ID or document. Unfortunately, many fake IDs and documents easily get past human scanners. New identification verification services, such as Samsung SDS ID Verification, apply forensic tests for fast proofing of documents, and catch fake IDs with greater accuracy than the human eye. With this service, organizations can scan, upload, and quickly authenticate identity documents including passports, driver's licenses, and identification cards. In addition, use of optical character recognition (OCR) and barcode decryption can extract identity information from the ID to pre-populate forms, helping accelerate the online application process.

Example: Open a New Checking Account or Apply for a Small Business Loan

- Alex fills out a new application on his smartphone
- He signs the application on his smartphone
- Alex is prompted to submit two forms of ID
- The application pulls his image and personal information from these forms of ID
- Alex then snaps a picture of himself and the app verifies that the image on the documents is the same as that of the person taking the picture
- Alex's application is approved



Secure Collaboration Services

New services enable institutions to easily assist and collaborate with customers completely online, providing greater convenience and streamlining the onboarding process. These collaboration solutions enable both the employee and the customer to move effortlessly between messaging, screen sharing, white-boarding, and real-time meetings to review, complete, and sign documents from any device, at any time.

Example: Conduct an Account Review

- An existing customer, Julia, has a question on an investment document that needs her signature
- Using her tablet & ID verification, she records her voice, highlighting and recording her question over the document
- Her investment manager, Mike, receives and listens to her questions
- He is easily able to record a response and sends it to Julia
- Julia is happy with the response and with being able to collaborate over documents digitally, just as they would in person
- Julia signs the document on her tablet and her account is updated

Signature Collection Services

Online notary services help financial institutions maintain a completely paperless process, while improving productivity and application close rates. Customers easily connect via webcam to a live notary—typically available 24 hours a day, 365 days a year—to electronically sign documents. The notary verifies and confirms a customer's identity and then applies a digital notary seal.

Bottom Line

New biometric authentication technologies that use fingerprint, facial, iris, and/or voice scans are setting a new standard for identity verification and data security. But without a parallel process to validate that a biometric identifier belongs to the real account owner, and not a criminal, biometric authentication fails to truly protect customers. Fortunately, the issue can be solved by combining the KYC identity verification and biometric enrollment processes. Additionally, new regtech solutions from leading providers such as Samsung SDS are enabling new ways to onboard customers completely online. These new services allow institutions to reshape traditional practices and the digital customer experience, ultimately helping them deliver a great user experience, increase revenue, and establish a competitive edge.

About Samsung SDS America, Inc.
Samsung SDS America (SDSA) is the U.S. subsidiary of Samsung SDS, a $7B global software solutions and IT services company. SDSA helps companies optimize their productivity, make smarter business decisions, and improve their competitive positions in a hyper-connected economy using our enterprise software solutions for mobility, security and advanced analytics.

Contact Us
To learn more about Samsung SDS America, Inc. visit www.samsungsds.com/us/en or email us at bd.sdsa@samsung.com.

[1] "Consumers and Mobile Financial Services 2016," March 2016, Board of Governors of the Federal Reserve Systems, 15 September 2017 <https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf>

[2] Boris Shiklo, "Mobile Banking: Exploring Trends for Market Leadership," 16 May 2017, Forbes, 16 September 2017 <https://www.forbes.com/sites/forbestechcouncil/2017/05/16/mobile-banking-exploring-trends-for-market-leadership/#1bb220ce6962>

[3] "2017 Data Breach Investigations Report," Verizon, 16 September 2017 <https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf>

[4] "Gartner Says the Internet of Things Will Drive Device and User Relationship Requirements in 20 Percent of New IAM Implementations by 2016," 15 December 2014, Gartner, 17 September 2017 <http://www.gartner.com/newsroom/id/2944719>

[5] "Biometric Smartphone Update," 2016, Acuity Market Research, 22 October 2017, <http://www.acuity-mi.com/BSP.php>

[6] "Biometric Smartphone Update," 2016, Acuity Market Research, 22 October 2017 <http://www.acuity-mi.com/BSP.php>

[7] "Barclays Rolls Out Voice Biometrics for Phone Banking," 1 August 2016, Finextra, 15 September 2017 <https://www.finextra.com/newsarticle/29245/barclays-rolls-out-voice-biometrics-for-phone-banking>

[8] Rory Cellan-Jones, "TSB to Roll Out Iris Scanning Tech," 20 July 2017, BBC News, 15 September 2017 <http://www.bbc.com/news/technology-40663365>

[9] "Gartner Says the Internet of Things Will Drive Device and User Relationship Requirements in 20 Percent of New IAM Implementations by 2016," 15 December 2014, Gartner, 17 September 2017 http://www.gartner.com/newsroom/id/2944719

[10] Heather Connon, "Know Your Customers: The Complexities Explored," April 2016, Deutsche Bank AG, 16 September 2017 http://www.gtb.db.com/insights-and-initiatives/flow/Know_your_customer_The%20complexities_explored.htm

[11] "2017 Identity Fraud Study," 1 February 2017, Javelin Strategy & Research, 16 September 2017 <https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new"

[12] "The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure," 2017, Capgemini Consulting, 17 September 2017 <https://www.capgemini-consulting.com/resource-file-access/resource/pdf/privacy-and-cybersecurity-in-fs_dti-research-report.pdf>

[13] Bob Sullivan, "Identity Theft Hit an All-Time High in 2016," 6 February 2017, USA Today, 22 October 2017 <https://www.usatoday.com/story/money/personalfinance/2017/02/06/identity-theft-hit-all-time-high-2016/97398548/>

[14] Dominic Mac, "The KYC and AML Landscape in 2017," 27 March 2017, Thomson Reuters, 22 October 2017 <https://blogs.thomsonreuters.com/financial-risk/know-your-customer/kyc-aml-landscape-2017/>

[15] "Retail Banking 2020: The Future of the Retail Banking Industry," 2014, PwC, 22 October 2017 < https://www.pwc.com/gx/en/banking-capital-markets/banking-2020/assets/pwc-retail-banking-2020-evolution-or-revolution.pdf>

[16] Graham Charlton, "Why Do People Abandon Financial Applications Online?" 14 December 2016, SaleCycle, 17 September 2017 <https://blog.salecycle.com/strategies/people-abandon-financial-applications-online/>