SAMSUNG SDS

Managing Security and Customer Experience with Biometric Authentication for Financial Services

NexSign Biometric Authentication

Table of Contents

Objective

This resource is for financial services professionals - CISOs, VPs of Information Security, Chief Product Officers, etc - concerned with security, customer experience, and identity verification. From the outset, we intend on setting the stage for challenges that banks and financial institutions face today. We'll then transition into a discussion regarding tools and methodologies that are available on the market to address those challenges. In closing, we'll introduce Nexsign, an enterprise-level identity authentication solution for the financial services industry.

Overview

The introduction of mobile banking options and the increasing number of digital transactions changed security requirements drastically for banks across the globe. Managing and authenticating customers is much more complex than it might have been decades ago when there was a very limited number of channels available to consumers for executing financial transactions. Now, with banks being forced to take an omnichannel approach, authenticating users and confirming digital identity is becoming a significant challenge.

From the perspective of the customer, it's of the utmost importance that all transactions being processed, regardless of where or when they're occuring, are vetted for authenticity and correctness. Digital identities are easily manipulated. 100% of fraud happens within authenticated sessions, and that is no coincidence. Outdated techniques like two-factor authentication that doesn't rely on behavioral or biometric modalities are easily penetrable by social engineering and phishing tactics. Customers want heightened security without sacrificing a fluid and intuitive banking experience.

That's where biometric authentication technologies come into play. There's no better way to ensure a secure digital environment without interruptions to the customer experience. Rather than prompting a user to enter their mother's maiden name, information that could be easily stolen from a user through phishing tactics, biometric modalities include fingerprint, iris, voice, and face recognition. These authentication points are unique to that user, and are monitored continuously behind-the-scenes to deliver a seamless experience coupled with the highest security standards.

About Samsung SDS

Samsung SDS is a global software solutions and IT services company. Their biometric authentication solution, Nexsign, offers fingerprint, facial, and voice recognition and offers behavioral, continuous, and risk-based authentication practices for best-in-class security and user experience. This solution has been utilized by a leading ATM manufacturer to streamline deposits and withdrawals in accordance with security best-practice, has been integrated with an enterprise software company's mobile API platform to enable its customers with biometric authentication within mobile banking software, and powers nearly 10 million authentications a day via Samsung Pay and Samsung Pass.

Challenges Banks Face Today

Rising Competition

It's not just customers' expectations that are rising. Investment in global FinTech companies nearly quadrupled from 2013 to 2015 - from $5bn to $20bn. These FinTech companies, like Stripe, SoFi, and Credit Karma, are now competing for market share with more traditional financial institutions. It's clear, based off research conducted by Kantar TNS for Quadient, that there is a need for traditional banking services. 56% of those surveyed stated that they don't want mobile banking solutions to completely replace traditional bank experiences. The challenge for financial institutions in 2018 is finding a balance between those two

> 56% of those surveyed stated that they don't want mobile banking solutions to completely replace traditional bank experiences.

consumer options. Banks need to accommodate users by providing both fantastic brick and mortar experiences in conjunction with frictionless and intuitive mobile banking options.

Accommodating Omnichannel Banking

Software and mobile banking options are being introduced everyday, and it's estimated that nearly 80% of users have downloaded a mobile-banking application to process transactions. Nearly 40% of respondents in the aforementioned survey communicated that they use their banking application at least once a day. The reality is that multichannel banking has been around for a while now. Customers have processed transactions via ATMs, call centers, and internet banking for years. Omnichannel banking incorporates an understanding of your user's preferences regardless of device. An omnichannel strategy enables financial institutions to gain insights into the users' behaviors making service in the future more personalized and impactful. The challenge for banks today is developing both the infrastructure and practices to ensure their users' actions and preferences inform the service they receive across all channels.

Keeping Up With Consumer Demands

Consumers have a tendency to extrapolate their experiences from other industries and organizations to all of their consequent brand interactions. For example, organizations like Amazon stress the importance of personalization and targeted experiences. Consumers get

> Raconteur reports that 69% of financial services customers would volunteer personal information for more tailored experiences and financial advice.

used to getting personalized product recommendations and expect that same kind of personalized experience as they shop with other digital retailers like Wal-Mart, Etsy, or Urban Outfitters. Raconteur reports that 69% of financial services customers would volunteer personal information for more tailored experiences and financial advice. It's clear that the vast majority of consumers desire tailored banking experiences, and are even willing to provide personal information to drive that experience. The challenge for banks is keeping up with other industries and consumer expectations around the customer experience.

Keeping up with competition within the financial services industry, developing an omnichannel banking experience for your customers, and meeting consumer demands for customized user experiences is no small feat. Meeting all of these requirements within a highly secure digital environment is even more challenging.

> Software and mobile banking options are being introduced everyday, and it's estimated that nearly 80% of users have downloaded a mobile-banking application to process transactions. Nearly 40% of respondents in the aforementioned survey communicated that they use their banking application at least once a day.

A Modern Security Solution: Biometric Authentication

Overview

Complicated mobile authentication processes with passwords, security cards, and one-time passwords (OTPs) are inconvenient to use and expose users to increasingly sophisticated attacks. These traditional identification methods impede users from seamless or frictionless user experiences by requiring manual entry, and oftentimes proper re-entry, of these details into forms and fields. This type of authentication is referred to as knowledge-based authentication and can expose both a user and a financial organization to unwanted risk. This traditional approach can still be valuable in conjunction with other authentication technologies, provided that it doesn't interfere with the user's experience.

Types of Biometric Authentication

- Fingerprint 
- Face 
- Iris 
- Palm 
- Voice 

> Prevent account takeovers and other cyber threats with contextual, cognitive and physiological user profiles that are created and monitored in real-time using deep learning and over 2,000 behavioral traits.

Using unforgettable biometric data, such as a fingerprint, face, iris, palm or voice, biometric authentication solutions deliver enterprise-grade identity authentication that is convenient, reliable and secure. Users aren't slowed down by manual entry of hackable factoids or passwords. Instead, they use their application or device as they normally would under the protection of continuous authentication using their palm, iris, facial features, or fingerprint as their "password". These modalities are specific to the user and are very difficult for unauthenticated users to copy or mimic providing for enhanced security.

Understanding Behavioral and Continuous Authentication

Behavioral and continuous authentication are closely related, and work together to provide ultimate security within a seamless experience. Behavioral authentication recognizes trusted customers and spots cybercriminals by establishing and analyzing "behavioral DNA" during an online session. Behavioral DNA is determined by monitoring over 2,000 behavioral attributes of any given user. It relies on monitoring the way a user interacts with both the software and the device being used. It then cross references new user inputs with the profile it has already built for that user based on past interactions. If something doesn't line up - maybe the speed with which they are typing on the digital keyboard - the session will be interrupted for further identity verification.

Continuous authentication technology runs silently in the background of any session, only prompting the user for security related information when necessary. If you consider KBA tactics discussed earlier, authentication steps are front-loaded towards the login phase of a user's interaction with any given application. Once that step has been passed, hopefully through legitimate means, authentication requirements are no longer in play. Intermittent authentication will interrupt the user throughout multiple stages of their session which is a terrible experience. That's not the case with continuous authentication technology.

Prevent account takeovers and other cyber threats with contextual, cognitive and physiological user profiles that are created and monitored in real-time using deep learning and over 2,000 behavioral traits. Accompanying behavioral and continuous authentication techniques with biometric authentication creates an extremely secure environment that only gets stronger with time.

Leaders in Biometric: Samsung SDS + Nexsign

Evolving Decades of IT Expertise Into Modern Fintech Security Solutions

Samsung SDS is rewriting the playbook for financial service organizations by providing innovative biometric authentication solutions for enhanced security and improved customer onboarding and retention.

Nexsign Biometric Authentication, a Samsung SDS offering, offers a comprehensive approach to identity verification and continuous authentication. Financial organizations can easily integrate Nexsign Biometric Authentication with their existing software, reducing costs associated with managing security across multiple channels and devices for employees and clients.

Nexsign Use Cases

Biometric Authentication In Action

1. **Securely and conveniently access mobile applications**
   A leading financial services and legal data provider implemented Nexsign biometrics for client access to its software solutions.

2. **Enhance authentication through biometrics**
   A global enterprise software company integrated Nexsign into their mobile API platform to enable its customers to include biometric authentication within their mobile applications.

3. **Transact without a bank card or PIN**
   The leading ATM manufacturer improved customer experience and mitigated fraud risk by using multi-factor, step-up biometric authentication.

4. **Support and protect users executing online transactions**
   Nexsign currently supports more than five millions users using Samsung Pay today.