SAMSUNG SDS

Streamlining the Retail Banking Customer's Experience with Seamless Authentication

Introduction

Retail banks are facing serious challenges in today's customer-centric world. With the proliferation of mobile technology, customers expect unlimited access and a frictionless experience. At the same time, fraud and data breaches are becoming more prevalent and dangerous. According to Kaspersky, in 2017 the industry experienced the highest percentage of financial phishing ever reported (1).

This increase in account takeovers result in fewer returning customers and decreased loyalty, costing banks valuable business. Technology is at the center of improving a bank's operations and security, both of which will positively impact the customer. Biometric authentication improves security and streamlines banking operations, leading to more loyal customers. Expedited banking experiences that utilize best-in-class security technologies will promote profitable retail banking.

Retail Banking Challenges

Nationwide, retail banks are facing similar challenges. Customers have no interest waiting in long lines for bank tellers or representatives who may not have answers to their questions or access to immediate on-site solutions. Customer onboarding can be burdensome and painstaking which creates a poor first impression. Knowledge-based authentication techniques are not only insecure, but also slow down the authentication process by requiring manual entry or communication of personal information. The list of challenges goes on and on.

Present-Day Retail Banking Challenges

- Meeting customer expectations regarding fast and effective service
- Quick and painless onboarding
- Unbreachable security measures for protecting personal and financial information

For years, banks have used security practices such as knowledge-based authentication for password protection. Knowledge-based questions are typically personal such as "What is your mother's maiden name?" or "What street did you live on as a child?". In today's world, this information is stored across the Internet and is often made accessible to those committing identity fraud through hacking or other means. Account takeovers lead to lost customers, bad press, and potential lawsuits under situations of negligence.

1. Financial Security Cyberthreats in 2017. Kaspersky, 2017, pp. 4–4, Financial Security Cyberthreats in 2017., https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07162608/Kaspersky_Lab_financial_cyberthreats_in_2017.pdf

Banks have tried to shift their approach to one that leverages more advanced technology for increased customer satisfaction through ease of use, simplicity, convenience and greater security. This includes mobile applications that require two-factor authentication, feature mobile check deposit, and are available to the user at all times of day. According to a 2017 eMarketer article, over 80% of mobile users have downloaded a mobile banking application to process transactions.

Technology is the driving force behind not only omnichannel banking, but also new security features to prevent account takeovers and improve the customer experience.

Many banks have turned to biometric authentication to give customers a more streamlined experience while mitigating fraud risk.

Introducing Biometric Authentication Technology

Biometric authentication relies on observance or capture of biological traits like fingerprint, voice, or facial structure. This new form of authentication eliminates the need for mixed-case alphanumeric passwords, security cards, and one-time passwords.

Mixed-case alphanumeric passwords add unnecessary complexity for the user, while failing to minimize account takeovers. Security cards are not always convenient and leave users exposed to highly-complex attacks. One-time passwords are usually delivered to devices through email or text message, two communication channels that could be compromised.

Through using a person's biological data, such as a fingerprint, face, iris, palm or voice, biometric authentication solutions deliver enterprise-grade identity authentication that is convenient, reliable and secure - ideal for both banks and bank account holders. Consumers can also use these modalities at ATM machines or for signing into mobile applications. These modalities are specific to the user and are very difficult for unauthenticated users to copy or mimic providing for enhanced security.

Biometric authentication adds a layer of security that is personalized to the user, minimizing the risk of account takeovers or fraud.

"Behavioral biometric solutions select from 20 unique features from its 500+ behavioral profiling metrics to authenticate a user." [(2)]

A truly seamless experience could also include behavioral authentication measures for enhanced security. Behavioral authentication analyzes behavioral DNA using thousands of behavioral attributes to discern the difference between trusted customers and cybercriminals. Behavioral DNA is established through user patterns such as their typing speed and how they interact with the application. Irregularities will prompt further authentication to ensure a secure environment. Continuous authentication is the process in which these irregularities will be intermittently challenged throughout the user's session on the application.

2. "What Is Behavioral Biometrics?" Behavioral Biometrics, Prevent and Detect Fraud, Biocatch, www.biocatch.com/resources/data-sheets/what-is-behavioral-biometrics.

Biometric Authentication with Samsung SDS

Customers are more likely to open and maintain an account at a bank where they know their information is secure and their time isn't wasted. Samsung SDS understands the need for financial institutions to have the best security to ensure customer data remains confidential, and banks remain fraud-free. As a result, Samsung SDS has launched a biometric authentication solution that enhances security and increases customer retention rates.

> Consumers want to choose how they interact online and Samsung SDS Nexsign is a platform that gives that choice.
>
> Frances Zelazny | Biocatch

In today's financial world, biometric authentication is becoming more and more prevalent. Use cases include a leading financial services and legal data provider implementing Nexsign for client access to its software solutions. In another case, a global enterprise software company integrated Nexsign into their mobile API platform to enable its customers to use biometric modalities to access their mobile applications. In addition, Nexsign supports and protects over 5 million Samsung Pay users today, allowing them to complete online transactions without worry.

Samsung SDS Nexsign Biometric Authentication is a cutting-edge fintech security solution that offers a comprehensive approach to identity verification and continuous authentication for maximum security. Banks with fraud-detection and identity-theft systems in place can integrate this software with existing technology. This new authentication system simplifies the authentication process while improving security, a win-win for both the banks and the consumer.

Biometric authentication gives your customers the added security they desire, while simplifying the process.

Learn More Learn more about how to incorporate these cutting-edge tools into your showroom.

LET'S TALK

Whether you are looking for a specific business solution or just need some questions answered, we are here to help!
Email: bd.sdsa@samsung.com Web: www.samsungsds.com/us/en Blog: www.samsungsds.com/us.insights/blog

/SamsungSDSA @SamsungSDSA

SAMSUNG SDS AMERICA SAMSUNG