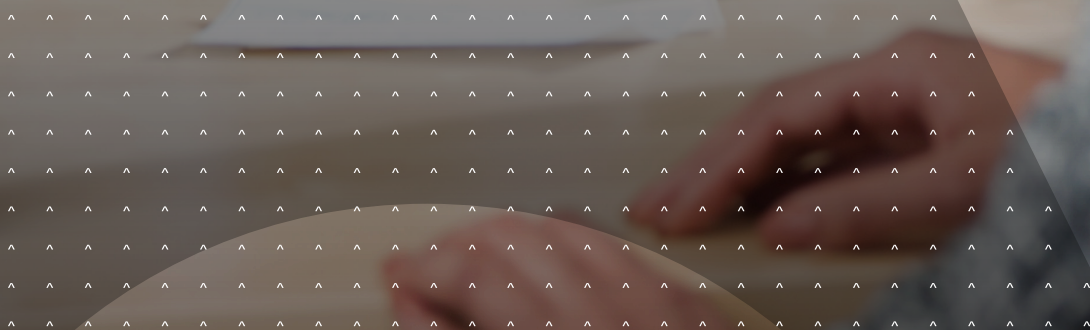THALES

Single Vendor Approach to Banking Security

Single Vendor Approach to Banking Security

As society becomes more technologically sophisticated, so does the way we manage and protect our money. Consumers are at the core of the banking industry, relying on the freedom to virtually connect from anywhere at any time.

Automated Teller Machines (ATMs), online banking and mobile banking apps have simplified financial transactions for consumers around the world, however not without ample threats in identity theft, fraud and data breaches. Thales, a global leader in digital security, is alleviating these stressors and safeguarding customer authentication for financial institutions.

Relying on traditional methods to protect one's finances and identity has become increasingly difficult. Authenticating a person's identity by relying on PINs, passwords, or the visual inspection of a driver's license or passports has proven ineffective, particularly with online transactions. Introducing biometrics and document authentication into the banking security eco-system provides added layers of security and efficiency both for the online environment and the in-person experience.

The Customer Journey: Account Origination & Loan Applications

Historically, when a customer opened a bank account, they took a trip to the bank of their choice where a member service representative would discuss their options, collect personal information, and manually inspect that individual's ID before setting up an account. With more banks existing solely online, such as Ally and Chime, and traditional banks opening online subsidiaries, like Finn owned by parent company Chase, account origination and even loan applications are now possible without customers having to leave the comfort of their own home.

Evolution of Customer Identification: In-Person vs. Securely Online

High end fingerprint sensors and quality cameras built into today's smart phones are allowing these online banks to benefit from increased security and efficiencies previously limited to face-to-face transactions. By incorporating Thales Cogent's state of the art biometric algorithms and authentication software, customers can verify their identity remotely. By simply taking a picture of their ID document, Thales' authentication software can authenticate the ID and capture the demographic information for error proof application completion. From there, users enroll some form of biometric such as finger, face or iris which can be used from then on for account access and identity verification.

While the concept and use of banking apps is certainly not new, the use of these technologies increases security as compared to the use of username and password alone.

How Does it Work?

Facial recognition technology, in collaboration with robust authentication software on a phone or embedded on an even more secure document reader, analyzes documents and compares the live person with the images on a document or embedded in a document chip to correctly cross reference and confirm a person's identity. This one-to-one verification process securely authenticates the person and their personal data prior to any transactions taking place. Advances in liveness detection have made this 1 to 1 verification process nearly impossible to spoof.

Coupling biometric verification with the ability to authenticate a driver's license or passport using Thales' high end Gemalto Document Readers, allows those financial institutions still providing face-to face services access to the same technology at the branch level. Banking branches will not disappear overnight and some people (especially those seeking loans supporting large expenses such as college tuition or a home purchase), will still prefer face to face assistance. The technologies Thales provides is equipped to support both online and in person use cases. In fact, the same fingerprint a customer uses to access their account using their mobile phone can also be used at the branch level using USB powered fingerprint scanners.

These fingerprint devices offer hassle-free, real-time identification at the bank counter. No smartphone required.

Physical Security Advances

Facial recognition can also be integrated into a bank's physical security systems and camera networks. Using the live feed from multiple security cameras linked to the same facial recognition database, banks can easily deploy face-in-the-crowd monitoring. By building numerous white lists (lists of known employees, vendors, etc.) and watch lists (lists of known fraudsters, banned individuals, etc.), a bank can consistently grant access to employees and monitor patrons, all while keeping an eye out for persons of interest.

Document Readers – Know Their Identity

We all know that identity fraud is a crime. Identity fraud and identity theft are used interchangeably as it pertains to an individual obtaining another persons' personal data and using it as a means of personal gain. Typically credit cards and ID cards/passports are involved as fraudsters gain access to personal data, such as Social Security numbers, bank and credit card accounts. The resulting costs of such activity are high, including out of pocket costs to the victim and bank as well as time and energy spent trying to rebuild reputations.

Card fraud and identity fraud are increasing globally and it's not just because card issuance is increasing. It's because fraud is actually outpacing growth. The fraudsters are getting better at using fraudulent cards in ways that card issuers and merchants can't detect right away. Mitigating risk and securing identities starts with Identity Document Verification (IDV), which seamlessly authenticates government issued documents using document reader technology.

Thales Gemalto Solutions to Capture and Authenticate Identity Documents

COUNTERTOPS   **KIOSKS**   **MOBILE PHONES**

Physical document readers provide unrivaled accuracy and speed by performing a sophisticated analysis of the presented document within seconds, testing for document integrity, checking for security features within the document, and reviewing for data consistency. For example, a Dual-Sided ID Card Reader, was designed specifically for use with ID-1 size documents (Driver's License size) to help mitigate fraud risk. Patrons can present their document in any direction and within 4 seconds, the analysis has been performed and returned to its owner. This smooth experience helps stop fraud, improve customer service and speed, automate authentication, and reduce human error, all at the same time. ID document readers can also be used in similar situations and have the added value of being able to read and authenticate multiple document types. They can also be easily integrated into kiosks for free- standing, self-service situations. What better way to enhance the customer experience and build their trust?

Streamlining Internal Processes

Even after minimizing the security threats externally, extra measures are necessary to ensure the security internally within the financial industry. Fingerprint-based background checks are used more and more each year to ensure clean employee criminal records. Utilizing commercial off the shelf (COTS) equipment, financial institutions are able to capture a potential employee's fingerprints in house and submit them to the state and FBI, for thorough background screening versus sending applicants elsewhere.

Conclusion

Thales' identification solutions, from document authentication to biometric verification, encompass all aspects of creating proactive security solutions in the banking and financial sector. Eliminating human error and introducing multi-factor authentication, increases security both internally and externally. Widespread adoption of such technologies will ultimately establish the groundwork to help alleviate security issues in the financial sector, and allow institutions to operate at a more efficient level.

Thales Gemalto Double-Sided ID Card Reader CR5400

Thales Gemalto OEM Document Reader AT10K for use in ATMs and kiosks