BANKING CUSTOMERS

Case Study: **Biometric Authentication**

INNOVATION HIGHLIGHTS

- Eliminate passwords
- Strong 2FA with possession and biometrics
- Proven performance with 3rd party validation

BENEFITS FOR FINANCIAL INSTITUTIONS

- Higher customer engagement and retention
- Compliance with identity regulations
- Reduce fraud
- Lower total cost of ownership (TCO)

BENEFITS FOR CISO

- Strong 2FA security with biometrics
- Easy deployment
- Lower support costs
- Secure storage of biometric templates

BENEFITS FOR HIGH VALUE CLIENTS

- Low-friction user experience
- Confidence that identity is protected
- Assurance that high value transactions have additional security measure via biometrics
- No passwords or tokens to remember
- Multiple individuals and multiple devices with access to the same account

An independent full-service financial services group for high net worth individuals wanted to eliminate passwords and PINs for their clientele. Native biometrics such as Touch ID, face, and fingerprint did not provide the level of security the firm needed. The firm also did not want to make customers jump through hoops to prove their identity. After an exhaustive RFP process, Veridium's solution was chosen for its superior security posture and performance.

THE PROBLEM

Balancing identity protection and user experience

The infamous bank robber Slick Willie Sutton reportedly said when asked why he robbed banks, "because that is where the money is." Financial institutions continue to be attractive targets, and unfortunately technology has made them more vulnerable to attacks. Financial executives understand the importance of developing innovative ways to protect the privacy and financial assets of their customers.

Those providing financial services to high net worth individuals also need to consider their clients' expectations for a frictionless experience. Mobile apps and online services are now the key points of customer interaction for financial institutions. This leads to overall rising expectations regarding the level of service from digital channels, including improved convenience and security.

Veridium's 4 Fingers TouchlessID outperforms other biometrics with a False Acceptance Rate of 0.01% and a False Rejection Rate of 1%

Case Study: **Biometric Authentication**

VERIDIUM'S SOLUTION

Frictionless experience

Veridium has the best mobile biometric on the market today – 4 Fingers TouchlessID. The user experience is sleek, and it works anywhere on any smartphone with no environmental constraints. The other biometrics considered, like facial recognition and voice recognition, had higher FAR (false acceptance rates) and FRR (false rejection rates) than Veridium. In fact, during performance testing, Veridium's FRR was 60% lower than the closest biometric solution. This was a critical criteria for the firm, because it didn't want legitimate customers treated like imposters and locked out their accounts. With Veridium, the firm felt confident that the low FAR (0.01%) and low FRR (1%) were within acceptable limits for interfacing with its high net worth customers.

Visual cryptography provides superior security

The VeridiumID platform uses a distributed data model to store biometric vectors. Using visual cryptography, the scanned biometric template is encrypted and stored partially on the customer's smartphone and partially on the company's secure server. This distribution makes it more difficult for an attacker to steal a complete biometric template.

HOW 4 FINGERS TOUCHLESSID WORKS

1 Place your hand behind your phone

2 The rear camera detects your fingers

3 Place them within the guide and hold your hand steady

4 All four fingerprints are captured at once

VERIDIUM
TRUSTED DIGITAL IDENTITY

www.VeridiumID.com
info@VeridiumID.com

London
Boston
New York
Oxford
Bucharest