Biometrics in Fintech for Security, Access

AUGUST 2018 TECH BRIEF FOR FINANCIAL SERVICES TALENT NETWORK

Fraud Protection through Unique Physical Traits

In recent years, the financial sector, of perhaps all sectors, has borne the biggest brunt of nefarious efforts to compromise client accounts, and steal assets, cash, and identities. Ongoing efforts by banks and other financial institutions to accommodate ease of access requirements preferred by clients, have been offset by the concomitant onerous security requirements, including convoluted password requirements, PINs, and frequent mandatory changes to same. While clients like the convenience of mobile apps, ATM's and online speedpay options, the maintenance requirements associated with the necessary security steps make the events themselves frustrating to execute.

The use of biometrics as a means to authenticate and secure account access for each user, based on their unique physical characteristics, is a promising method that could give consumers the ease of account access they desire, while giving the financial institutions that support these access methods, the security and regulatory compliance they must have.

Challenges continue based on standards, or lack thereof, and expense to implement, but the direction towards the use of biometrics in this space is undeniable, and banks and financial institutions need to have these technological imperatives included in their strategic plans.

Labor Force Takeaway

The biometric technologies currently in production (or in development) are very new and many are still in beta mode. Certifications needed to support deployment of these technologies at the user level will likely be platform and equipment specific; likely, there will be certifications provided by each manufacturer, much like they are in healthcare, where reading and interpreting machine imaging of human physical characteristics is commonplace. Electronics certification to support equipment maintenance (CET-a certification, ESA, and Journeyman CET) could be of benefit to associates who, as part of IT support, will be charged with maintaining reader functionalities.

Randee Jennings, **jennings@njit.edu**, Technology Advisory Network Director for FSTN

Bypassing Password/PIN Authentication Issues

For many years, as the financial sector has reengineered to provide more convenient access to client accounts, the security requirements necessary to safeguard client assets has proven to be challenging, both to implement and to maintain, for banks and customers alike. The information used for protection – specifically, passwords and PINs, - is often not well managed by clients, who make them as easy as possible for themselves, and is guessable, able to be compromised. The credentials themselves, the structure of which is managed by the financial institution, is often required to be challenging, accordingly, to prevent their defeat. And compliance requirements, across all institutions, is still not yet standard, making ubiquity impossible.

Identity, security and trust are fundamental to payments, commerce and finance, especially in an increasingly digital economy. The battle against cybercriminals is real and ongoing. Technologies like biometrics will help authenticate customers, secure transactions, and mitigate fraud losses.

Biometrics is the most promising technology to resolve these issues. It allows for simple quick account access, but with the requisite uniqueness to render hacking and compromise difficult if not impossible.

There are at present five biometric types under exploration for development and promulgation:

(1) Iris Scan
   a. Best combination of security and cost competitiveness
   b. 200 points of data make replication nearly impossible

(2) Voice Recognition
   a. HSBC is already moving in the direction of voice recognition
   b. Issues faced with hackers using voice recordings
   c. Methods being developed to ensure recording use is detected

(3) Facial Recognition
   a. Issues – can't have blockage in the way (glasses, jewelry)
   b. Issues – Hackers using a life size photo
      i. Requirement to blink at a set interval can overcome

(4) Fingerprint Scans
   a. Least reliable
   b. Fingerprints fade in older clients

(5) Vain Patterns
   a. Palm, finger or eyeball
   b. Low false positives, but high cost to implement

Multimodal biometric platforms most secure. The key to success in this area is to innovate and integrate, however, a lack of agreed upon standards across the entire financial sector will make cross-institution usage challenging.

There are big savings to be enjoyed, however. In a recent study completed by the Forrester Consulting Group, a blind test bank implemented a biometric system for account access that saved the company over $24M over three years, mostly in fraud prevention, and client satisfaction. A 191% ROI was achieved as well.

A number of companies are in this space, including BloConnect, GSMA, Eyeverify, Daon, Findbiometrics, and IRC innovation, can provide demos and guidance on including biometrics in your strategic plans and budgets.

Randee Jennings, **jennings@njit.edu**, Technology Advisory Network Director for FSTN