Biometrics On All Fronts

by Steve Brown

You would think that a central bank would be one of the most secure and technologically sophisticated institutions in the world. That's why it was interesting to see a couple of months ago that hackers had breached the Bangladesh Central Bank's money transfer system. Once online, they posed as Bangladesh officials and submitted multiple requests to the New York Fed to have money within "their" accounts to be transferred to banks in other countries. Their efforts were successful, to the tune of $101mm. That is, until a misspelling in their final request of the word "foundation," spelled "fandation," raised a red flag at a routing bank and prompted a query of the transaction. Fortunately, $20mm of the money that was routed to a Sri Lankan bank was not immediately disbursed and was recovered. The other $81mm however, was sent to several accounts within a Philippine bank and stolen and the money has yet to be recovered. While Bangladesh's finance minister initially said he was considering a lawsuit over the matter, the New York Fed followed correct protocols for authenticating the payment instructions it had received from the SWIFT messaging system. It has since been determined that hackers were able to tap into the Bangladesh Central Bank's system because it did not have a firewall and had relied on cheap $10 second hand routers to connect its global banking network computers.

The ease with which hackers were able to walk away with literally millions of dollars made us think about the increasing sophistication of bank theft. While old school bank robberies like those pulled by Jesse James and his band of outlaws declined, banks still must remain diligent about security on all fronts. Banks these days must be wary of online fraud, to the various forms of theft that still take place within branches.

Fortunately for the banking industry, the sophistication of technology can now be used for dual security efforts both online and in the real world. Some banks have begun experimenting with biometric sensors that can actually identify customers who are significantly stressed (and who may be up to no good). By measuring an individual's blood pressure and body heat without their knowledge, biometric sensors can help banks identify unusual patterns that may signal that an individual is getting ready to attempt a robbery or is in trouble themselves.

Similarly, advancements in voice recognition software are enabling banks to authenticate customers faster and identify fraudulent calls from the bad guys. Voice authentication uses methods that can identify close to 130 individual characteristics unique to each person's vocal pattern and the large banks have begun rolling this security advancement out to customers.

Citibank is one of those banks and has embraced voice biometric and other security measures as a way of authenticating customers without the need for passwords or answering a series of personal questions when calling. Once customers provide an initial sample of their voice, any time they call, their voice is automatically matched to that sample to verify their identity.

Other biometric security measures banks have begun using include fingerprint and iris or eye scans. These can all be used to verify account owners through mobile devices quickly and easily. Eventually, they will likely also replace pin-based cards ATMs have long relied on to provide secure access to accounts.

While many biometric tools are still in the nascent phase and continue to be developed, combining these measures with increasingly sophisticated software allows banks to launch multi-pronged attacks on fraud and theft.

Banks these days are moving to combine layered defenses through biometric advances, branch sensors, software that scans data streams looking for unusual patterns, and even software that aggregates data from a myriad of sources for comparison. These are good ways to enhance the work of staff and make it harder on the bad actors, but as bankers know, the work will continue because the thieves are many and it only takes one to get in and steal money from the bank.

BANK NEWS

M&A Activity

1) State Bank and Trust Co ($3.5B, GA) will acquire S Bank ($109mm, GA) for about $11mm in cash (50%) and stock (50%), or roughly 1.02x tangible book. 2) First-Citizens Bank & Trust Co ($32.1B, NC) will acquire Bank of Virginia ($348mm, VA) for about $35mm in cash.

Hacking Risk

Given so many bankers and small business customers leverage LinkedIn for business, it is important to know that hackers are selling 117mm LinkedIn passwords on the dark web. Hackers will likely use such data to mine it and then gain access to email and bank accounts (because so many people reuse passwords all over the place). Alert your teams, change passwords and be careful when processing activity for clients as some may have been compromised.

Tech Expansion

Bank of America said it will expand its card-less technology to over 5,000 ATMs by the end of this year, as it seeks to leverage consumer usage of mobile devices. The technology allows customers to withdraw cash, make account transfers and check account balances using a digital wallet on their smartphones.

Inside Ally Bank

The bank reported as of Q1 that it has about 1.1mm deposit customers which break down 36% Millennials and about 32% each for Baby Boomers and Gen X.