Transforming Interactions

By Robert Capps, Vice President of Business Development, NuData Security

Automated banking will be the next big disruptor for the banking sector as traditional interactions with customers transform so that the in-branch banking experience will become much like the online experience. With a wide variety of alternative payment systems and cyrptocurrenies emerging such as bitcoin, there will be less need for customers to actually access a bank branch. One of the major impacts from this disrupter is that 30% of bank jobs could be lost before 2025 due to banking automation according to a study by Citigroup.

On the flip-side, alternative payment systems, virtual currencies and crowd-funding are pushing financial institutions to innovate or risk losing market share. Banks are already integrating more tools and solutions to make this a reality and it will become easier and easier to bank and pay online with favorite apps. Customer experiences will continue to improve with the aim to become faster and friction-free, while improvements in authentication become better at solving online user verification.

Authentication: The Big Challenge for Banking Automation

As technologies evolve for financial institutions, so will authentication, due to the pressing need to accurately identify customers and prevent fraud. Traditionally, only a driver's license and other photo ID would be all that was needed to verify the identity of the customer. Now however, the process of authentication has become much more complex with the advent of cybercrime and identity theft. Up to $1 billion dollars has been stolen over the last two years from financial institutions worldwide due to cybercrime.* Card-not-Present fraud alone is estimated to jump to $7.2.billion by 2020 according to the Aite Group. Identity fraud has resulted in cybercriminals stealing $112 billion in the past six years which equals on average about $35,600 stolen per minute according to the Javelin Group.* Cybercriminals have leveraged outdated security technologies employed by banks and financial institutions with an arsenal of techniques to strip banks, credit unions, financial institutions and consumers out of their money. Automation requires more interconnectivity and interactions between banking systems and before automation can truly evolve, the customer authentication problem must be solved.

The Advance of Behavioral Biometrics

Some of the most promising technologies in this space are also the most disruptive. They require internal organizational behavior changes as well as innovative technologies. Using advanced authentication models that use behavioral biometrics in a layered approach to verify that the person accessing or applying for an account is who they say they are, is one approach to help identify if the customer is really who they say they are. Just analyzing geographic locations, IP addresses, device ID, etc are no longer enough. How someone holds their device, the weight of their key strokes along with hundreds of behavioral data points are needed to verify that there is a human, and is the right human behind the transaction and that the behavior observed in the session is consistent with their profile. So even if another person

steals a device and tries to access an account or open a new one with a stolen identity, the technology will note that various biometric behaviors are not the same. Combining behavioral analytics and passive biometrics will go a long way towards ensuring fast and safe transactions for customers of banks and credit unions, while fighting fraud and meeting compliance standards.

Physical Biometrics Not the Panacea

Many banking and financial institutions are now adopting biometric approaches to identify customers such as selfies, fingerprints, facial and retinal scans. While these technologies have a place in the authentication stream, and are definitely and improvement over the old username and password, they do have some drawbacks to consider. Physical biometric authentication is not always situationally or culturally appropriate. For example, using voice recognition while in a meeting, or facial scans while at the theater. Some biometric data can be socially engineered, for example when Angela Merkel's photo was used to unlock a iris biometric test at a security conference. Fingerprints can be stolen from doorknobs and glass, and high resolution photos of faces can be taken from great distances and from video. Additionally, customers will not be able to change their fingerprints, facial or retinal information should this data be stolen and it is only a matter of time before they are. Once the data is stolen and sold on the Dark Web, the risk will persist over the person's lifetime.

Given that biometrics are being deployed for the most stringent of authentication tests such as immigration and banking, it will make this biometric data very desirable to hackers. We should expect more attempts by hackers to capture this data. The benefits of passive biometrics are that they are not stored nor is it possible to replicate them in any way, so there is not a chance of having personal behavioral biometrics stolen.

The Compliance Landscape

US Regulators have implemented new cybersecurity initiatives for banks and financial institutions that will require advanced technologies to meet the new regulatory environment. Insider threats as well as cyberthreats will be harder to perpetrate with evolving automated systems that will make it easier to detect and stop fraud. Technology will not be the only answer; sharing responsibility across the industry by participating in threat intelligence is another proactive step. Just this year, eight of the largest US banks have formed a group to tackle the growing cyber threat. This new group is expected to not only share intelligence about threats, but also prepare comprehensive responses to attacks as they occur and conduct war games designed for the issues facing the biggest institutions.

About the author:

Robert Capps is the vice president of Business Development for NuData Security. He is a recognized technologist, thought leader and advisor with more than 20 years of experience in the design, management and protection of complex information systems – leveraging people, process and technology to counter cyber risks.

*http://www.thisismoney.co.uk/money/saving/article-2955442/Banks-hit-largest-cyber-crime-mercy-hackers.html#ixzz4QBLjlpZl
Up to US$1billion - £650million - has been stolen in approximately two years from financial institutions worldwide.

*https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point
Identity fraud is a serious issue as fraudsters have stolen $112 billion in the past six years. That equals $35,600 stolen per minute, or enough to pay for four years of college in just four minutes.

*http://www.wsj.com/articles/credit-card-scammers-embrace-online-shopping-1477387802
Aite Group LLC, another consulting firm, estimated in May that so-called card-not-present fraud will rise to $4 billion this year from $3.2 billion in 2015. It expects that figure to jump to $7.2 billion in 2020.