waterstechnology

Biometric Technologies: The Identity Layer

The use of biometrics and identification technologies has skyrocketed within retail banking and has become an intrinsic part of the latest technology devices. But now the financial-markets industry is latching on to the potential of these technologies, once deemed science fiction, to strengthen and build out their security systems. By Josephine Gallagher

NEED TO KNOW

- The last 10 years have seen the uptake of biometric technologies across the financial services and tech industries, and now investment firms are beginning to unlock the potential of these technologies as a layer of defense.
- As the technology becomes more sophisticated, firms are using AI and machine learning to create digital models of individuals using behavioral biometrics.
- Once biometric security systems are breached both the individual and the technology are compromised. Unlike traditional forms of security, it is not a matter of resetting a password.
- At a time when the industry is experiencing an explosion of data, and firms are struggling to meet GDPR requirements, new questions are being raised surrounding the ethical use of biometrics data and the regulatory implications.

Identifying a person using biological data like fingerprints, facial features, voice, signature, or iris patterns was once a futuristic idea. Not only are biometrics widely used today, recent developments have taken the concept further and it is now possible to verify identities not only by physical attributes but also behavior.

Cyber criminals are becoming more sophisticated and their attacks more frequent, leading capital markets firms to follow in the footsteps of retail banking and tech giants, such as Apple, Google, and Microsoft by integrating these identification technologies into their security systems.

Matt Palmer, senior director at consultancy Willis Towers Watson, says traditional passwords are no longer a sufficient means of security on their own and that financial firms are quickly realizing the potential of biometrics.

“We have had 10 years of investment in biometrics [in the retail and consumer space], and the results of that are fairly mature systems to identify people—via voice, or fingerprint, or other means—that are now becoming embedded in business processes for large institutions, and beginning to replace the reliance on simple passwords and two-factor authentication,” he says.

According to a MarketsandMarkets report, published in July 2018, the biometrics industry is expected to grow to $41 billion by 2023. Security enhancements, however, are not the only reasons for the uptake in biometric technologies. Convenience, latency and user-friendliness have also led to the surge in the adoption.

Erik Kaland, COO of Stockholm-headquartered Storebrand Asset Management, says that although the latest identification technologies are more suited to the retail market and financial services, “getting rid of all that friction through biometric technology or near field communication (NFC) is key to succeeding” within the capital markets space.

Behavioral Biometrics

Cross your arms. Now cross them the other way. The second way wasn’t as comfortable, right? This was the explanation of behavioral biometrics given by Howard Edelstein, chairman and CEO of BioCatch, a provider of software that tracks such identifying traits.

He says each individual has thousands of cognitive micro-preferences that they are unaware of. Due to significant development in analytical technologies and artificial intelligence (AI), these preferences can be used to create a digital model of a person and their innate behavior, when accessing work PCs or databases, inputting data, communicating with counterparties, executing orders or authorizing executive-level decisions, to name a few examples.

“The whole notion of behavioral biometrics is to model you—the individual, the person—and authenticate you against your credentials that have been given to you by a bank or a financial institution,” says Edelstein.

Using biometric sensors, firms can create a profile of an individual from their mouse movements and keyboard strokes. This is then tracked and monitored to ensure all activity is carried out by the authorized person. The behavior of the individual is repeatedly sampled every few seconds.

Biometric technologies establish what is called a confidence and risk score to determine if an individual is who they say they are. This is often multi-factored in high-security circumstances where a person could be asked to provide multiple forms of identification such as a fingerprint and voice authentication, which could then be layered with behavioral biometrics.

“With a password it is black-and-white,” says Tower Willis Watson’s Palmer. “Either the password is right, or the password is wrong. That’s all there is to it. When we talk about biometrics, we are no longer in that black and white world and instead we are talking about confidence and risk.”

Given the volumes of data being pumped into security systems to identify, detect and monitor biometric indicators, financial services firms are turning to AI to power these capabilities. This is done using machine learning and deep neural network technologies, where the AI engine processes vast amounts of historical biometric data and learns the specific parameters that constitute as a high confidence score as possible for a person’s identity. With each encounter the AI technology will continuously learn about the biological and behavioral factors that make up the individual.

“If you consider biometrics, it is a technique of what we want to imply,” says Sriraam Malavalli, senior technology executive and consultant at Synechron. “Artificial intelligence, machine learning, data science or data alchemy is like a vehicle in order to achieve that.”

The perks of using biometric technologies are evident. They offer additional layers of defense that largely don’t disrupt a client’s day-to-day workflow. But now, as banks and investment firms are beginning to incorporate these technologies into their security infrastructures, sophisticated cyber criminals are keen to exploit their inherent weaknesses.

Code Red

In a traditional scenario, where an unauthorized individual accesses an account, it can take a matter of minutes to simply reset a password. In the case of biometrics, where someone manipulates a person’s identity, the reality is both the individual and the security system are compromised. Palmer explains that there are two ways in which biometric security systems can be breached: replicating the identifier, or bypassing the technology itself.

He says sophisticated cybercriminals can lift an individual’s fingerprint from a glass, for example. Over the years, security experts have demonstrated the vulnerability of security features based on single-factor biometrics. During a Mobile World Congress in 2016, Vkansee, a mobile security company, used Play-Doh to replicate a fingerprint to breach an Apple iPhone’s ID system within six minutes. Another infamous example stretches back to 2002 when Tsutomu Matsumoto, a Japanese cryptographer, fooled a fingerprint sensor using a gummy bear, a fingerprint taken from a glass and a digital camera.

“All static biometrics are spoof-able to one degree or another,” says BioCatch’s Edelstein. “What you know and what you have is kind of last year’s battle; it’s static, and anybody can have your identity if they want to have your identity, and everyone could know your secrets if they want to know your secrets.”

Palmer says cybercriminals can equally bypass a security system by compromising an internal member of staff to access a system. The idea is that deploying biometric systems requires a systemic approach to security, whereby firms should incorporate this layer of defense at all entry points. This involves having multiple identifiers across an organization, such as authenticating and authorizing the likes of clients, internal employees and third parties.

Biometric technologies were introduced to provide an additional line of defense and protect

unauthorized use of data. But given the intrusive nature of the technology, firms are presented with a unique set of challenges surrounding data ethics, as well as regulatory implications.

“There is a need for stronger regulation and legislative oversight as to how this data is used,” says Palmer. “We are addressing one risk and replacing it with another and that requires a very high level of maturity in order to secure that information.”

Data Troubles

Biometric security systems require large volumes of personalized data that can be used to identify a person by their physical features or behavior. The information gathered can also include biological characteristics such as heartbeat, venal structures in their fingers, or iris patterns. This information is then fed into AI engines, where the machine learns about the individual and creates an electronic model of each person.

By nature, deploying such security systems within a workplace can be invasive for those involved. This has raised questions over its limitations and whether consent should be obtained from those participating, similar to how firms require consent to use personal data under the EU’s General Data Protection Regulation (GDPR), which was implemented on May 25.

Bloomberg has been an early adopter of biometrics, launching two proprietary authentication tools in 2004—a finger image sensor on the Bloomberg keyboard, and B-unit, a portable credit card device. Phil Vachon, a security architect at Bloomberg, says that the two biggest challenges involving the technology include ethics and regulation. As many issues surrounding its regulatory scope have yet to be addressed, he says financial firms have a responsibility to carefully protect this personal data and respect those involved.

“There are a lot of open questions about the regulatory piece that have yet to be answered. As a firm you have to take a very conservative approach to how you deploy these technologies, especially in this jurisdiction,” he adds.

Other issues relate to the risk of storing such data within banks or investment firms themselves, or whether third-party providers are more equipped to manage these requirements, through mechanisms such as encryption. However, this introduces questions surrounding the consent of offloading these services to vendors, and the residual responsibility of the financial firm. As a result, the gathering of biometric data will likely make firms a more appealing target for sophisticated cybercriminals and organized crime.

“Once you start recording this data it becomes extremely valuable, and we also see some targeted attacks,” say Palmer. “Because if you have this type of data that is extremely valuable, that effectively can’t be undone, as it’s permanent security, and it can become a permanent weakness when it is compromised.”

Just the Beginning

As of now, the technologies inside trading systems have yet to mature and firms will require a level of readiness to replace legacy systems that are reliant on passwords and two-factor authentication.

Before this occurs, firms will need to consider issues regarding deployment and usability. The integration of biometrics systems will require a significant level of education and an onboarding process for those impacted. Additionally, many participants involved may be unable to use the technology itself depending their physical circumstances.

“So there is a rule of thumb that I follow from my experience: About seven percent of a user base of biometric technology is going to have a hard time with this technology,” says Bloomberg’s Vachon. “For example, when using fingerprint authentication, a user might have damaged finger prints because of an accident. And different sensor technologies behave differently with different skin types, which can impact the user’s ability to authenticate.”

Despite that, adoption of biometrics is under way. With an increase in remote working and the shift to cloud services, firms are seeking new and convenient ways to enable frictionless ways of working. One example of this, which has shown to be successful, is the use of biometric signatures to confirm transactions transferred to and from datacenters and cloud networks. This creates a digital archive of large contracts such as an Isda master agreement between over-the-counter market participants.

“We establish those cloud services within those regions with a specific signature,” says Malavalli. “So all these signatures hold a validation to say ‘I can, or can’t, move this data over to any other network or any other cloud movement setup.’”

While flawed, biometric technologies can serve as one piece of an overall line of defense, so long as it’s managed correctly. Andersen Cheng, CEO of Post-Quantum, a provider security technologies, says it is crucial for firms to mix and match various methods of authentication to meet an optimum level of security. He says this can include factors like “what you know, what you have and what you are,” which boils down to a password, static biometrics and behavioral biometrics.

“Using just one biometric or factor is very risky and you need to combine it with other factors,” he says. “If you mix and match it becomes more difficult for an attacker.”