Digital Banking

Biometrics: the Future of Mobile Payments

Nathaniel Karp

- **Benefits from biometric authentication extend beyond improving security**
- **Its adoption rate will continue to surge, particularly in the financial sector**
- **Biometrics has potential to transform the mobile payments system**

Security

The increasing usage of Internet, mobile devices, Wi-Fi, and cloud computing continues to expand the frontier of products and services available to billions of people around the world, with the potential to significantly enhance well-being even in the most remote areas of our planet. However, this has also multiplied the threats from security breaches, prompting more advanced methods of authentication and verification such as biometrics.

Over the past few years, cyber-attacks have grown in size and virulence, reaching critical industries such as banking, utilities, and airlines, as well as other sectors like retail, entertainment and hotels. In addition, the attacks have targeted governments and the military, escalating national security concerns. The damage includes job losses as the economy diverts resources to activities that provide lower value, disincentives to innovation by eroding the returns on intellectual property, and destruction of commercial activities due to losses of confidential information and market manipulation. In addition, the economy suffers from higher opportunity costs or reduced value-added from foregone activities as a result of lower investment in R&D, higher spending on network defenses and risk-averse behavior from consumers and businesses. Moreover, cleaning up cybercrime can reach significant amounts, particularly when the damages affect the brand, reputation and, customer retention and satisfaction.

According to the Center for Strategic and International Studies (CSIS), the cost of cybercrime to the global economy is around $450bn. Moreover, the Ponemon Institute reports that in 2013, 43% of U.S. companies experienced a data breach. At the individual level, the biggest risks are identity theft and loss of confidential information. The CSIS estimates that in the same year, there were 800 million individual records stolen around the world. In South Korea, for example, more than 70% of individuals aged 15 to 65 years had their personal data stolen and credit cards compromised in one month. In the U.S., according to a 2012 survey from the Bureau of Justice Statistics, identity theft affected 16.6 million people with a cost of $24.7bn in financial losses.

Biometric Banking

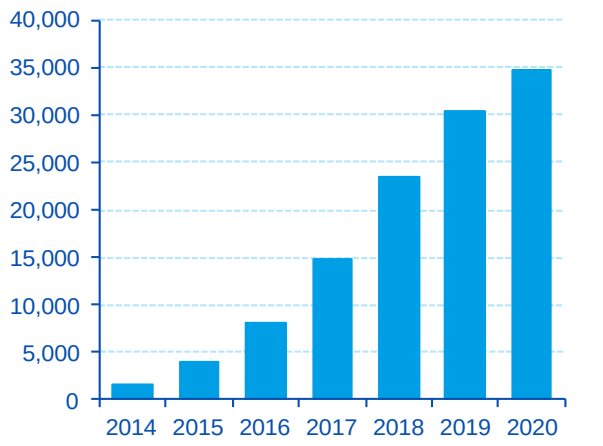
In response, a wave of innovation and capital has centered on developing new technologies to protect individual data and enhance customer experience. One option that is growing at a fast pace and shows great potential is biometric authentication. In essence, biometrics uses physiological and behavioral characteristics like DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, vein and signature patterns and hand measurements for the purposes of authentication and verification of human beings.

Despite elevated uncertainty on how the biometric market will evolve in the next few years, expectations are positive. For example, Acuity estimates that by 2020, biometrics will be used to authenticate almost 65% of all mCommerce transactions. In addition, global mobile biometric revenues are expected to increase to $34.6bn

from $1.6bn in 2014, with 35% being authenticated via mobile devices and 65% via apps downloaded by consumers. Other estimates indicate that the global biometrics technology market will reach $22bn by 2020, up from $11.2bn in 2015 and $4.2bn in 2010. In the financial sector alone, the market value could reach $8bn by 2020.[1] This includes biometrically-enabled smart mobile devices, biometric sensors, biometric app downloads, direct purchase and software development fees, and authentication fees from biometrically secured payment and non-payment transactions.

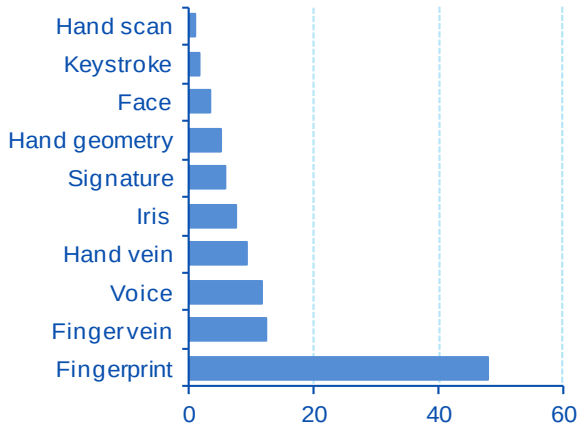
Biometrics is not uncharted territory for the financial industry; banks have explored options such as fingerprint scanning for decades, but the convenience and proliferation of mobile devices is making biometrics accessible to anyone with a smartphone. Fingerprint recognition has historically been the preferred option in the financial sector given its high accuracy and low-cost. A 2012 survey among 121 banks using biometrics revealed that 48% prefer this technology. Nonetheless, other technologies that fall under the *contact less* category, such as voice, iris, vascular and facial recognition are gaining ground and will provide greater versatility and convenience. In any case, this implies that the era of physical –cards- and logical –PINs and passwords- security measures may soon be over; providing the opportunity to develop a more integrated environment, where users can easily access a multiple range of products and services in a seamless fashion.

Chart 1
Mobile biometric revenue, $millions



Source: Acuity

Chart 2
Usage of biometric technologies among banks, %



Source: Biometix

Benefits and Challenges

For banks and customers, the usage of biometric authentication delivers significant benefits. First, it provides competitive advantages as better security increases trust, which represents the backbone of the business model. For example, biometrics can strengthen proof of identity processes, enhance fraud detection and improve identity management. Second, biometrics boosts customer experience by simplifying access, speeding processing times and facilitating a multichannel environment. Third, the combination of biometrics and other technologies can improve transparency, data analytics and real-time risk assessment. Finally, biometrics increases efficiency by lowering costs, improving internal controls, and facilitating audit trails and regulatory

1 See for example MarketsandMarkets, 6Wresearch and Visa

compliance. For example, biometrics provides an efficient way to comply with Know-Your-Customer requirements, which are aimed at curbing identity theft, financial fraud, money laundering and terrorist financing.

The increasing adoption rate of biometrics in the financial sector seems inevitable. A survey from Telstraglobal on Generations X and Y (born 1966-76 and 1977-1994, respectively) indicates that more than half of respondents value trust as the most important driver of choice when selecting a financial services provider. One in five individuals would share their DNA to help secure financial and personal information, while up to one in two are willing to pay for mobile identity. In addition, less than half are satisfied with their institution's security performance, more than a third have experienced identity theft, 40% of victims believe it was the institutions' fault, and 65% of them are likely to defect as a result.

Biometrics in banking is most popular in developing economies in Asia, such as India and Indonesia. In fact, this continent accounts for 52% of banks using biometrics worldwide. The Americas ranks second with 32%, followed by Europe (9%), Africa (6%) and Australia (1%). Across industrialized countries, Japan ranks at the top supported by a network of over 80K biometric ATMs and more than 15 million customers. These differences may reflect higher regulatory hurdles in the U.S. and Europe, associated with strict personal data protection rules.

Moreover, financial institutions and regulators in advanced economies have been cautious to implement biometric authentication as litigation costs and other damages caused by information leakages in centralized databases could be devastating, particularly if security breaches compromise operations in other industries or government agencies. For example, after an attack occurs, banks can issue new credit cards but are obviously not capable of replacing fingerprints. Likewise, if a credit card is compromised the damage is to the customer and the bank. However, if biometric information is hacked, it can be used on a wide range of activities outside the payment system, causing significant losses across the economy and turning into a national security concern.

Other challenges relate to lack of standardization to validate the security of biometric data for payments, as this creates barriers to interoperability when multiple vendors or business partners need to be integrated in the production chain. Nonetheless, ongoing innovation as well as industry and government initiatives can help advance the use of biometric technologies, mitigate the risks of centralized databases and develop domestic and international standards.

Bottom Line

Biometric authentication will continue to grow at a fast pace creating new business and employment opportunities, while transforming payment and non-payment transactions. Rapid adoption is allowing banks to boost security, enhance the customer experience and improve efficiency. New developments will provide additional benefits such as creating a fully integrated multichannel environment and across industries in a seamless fashion.