Shifting shape of banking biometrics

Tinna Hung, EyeVerify

2016 was a tipping point for biometrics in financial services, with dozens of banks worldwide launching biometric technology for customer authentication, typically via a single modality. And judging by the millions who have set up a biometric template, customers are increasingly accepting biometrics as a convenient yet secure method of logging in to their accounts. Financial institutions, meanwhile, are accruing benefits in increased customer satisfaction and engagement. Yet the biometrics story for financial services is far from complete. As customers conduct more of their banking on mobile, and as businesses move to digital and mobile banking, the nature of how biometrics is used in this industry will shift again.

To understand how the use of biometrics could evolve, it is important to understand why biometrics are being implemented in the financial services industry in the first place. There are two main drivers: security (real and perceived) and convenience. Yet while mobile banking is fast becoming the new norm, crucially there continues to be a segment of consumers who do not trust mobile devices for financial services. The same can be said for mobile payments, although the larger adoption barrier here remains availability at the point-of-sale. According to a recent study by Oxford Economics, more than half of respondents believe mobile money is less secure than cash\(^1\). Banks are addressing these security concerns via biometrics, which are increasingly in demand. The same Oxford Economics report notes that consumers are more likely to use mobile money if biometrics are offered.

But the security issue extends beyond consumer perception. The reality is that as mobile is used more for banking and commerce, mobile fraud also increases. RSA Security found that fraud originating from mobile increased from 10% of total fraud attempts in 2013, to 50% in 2015\(^2\). In addition, the number of data breaches is on the rise. Billions of credentials were stolen in 2016, and the problem is compounded by the fact that most people re-use passwords across multiple accounts, putting their data, including banking data, at risk. Biometrics mitigate this threat.

"Customers are starting to demand biometrics. Visa Europe found that 37% of European men would switch banks if their existing financial institution did not offer biometrics”

On the convenience side of the equation, passwords aren’t just insecure, they’re difficult. Complex passwords are hard to remember and provide for a miserable user experience on mobile thanks to small keys and the need to shift between two or three keyboards, multiple times if the password is properly complex. In contrast, biometric solutions have clearly evolved to the point where they are very easy to use – a quick scan of a finger, face or eye gives the user access to their account.

This convenience results in more frequent engagement and higher satisfaction. Digital Insight, which provides mobile and online banking infrastructure to hundreds of financial institutions in the US, says that people using Touch ID for mobile banking log in 26% more often\(^3\). In fact, customers are starting to demand biometrics. A study by Visa Europe found that 37% of European men would switch banks if their existing financial institution did not offer biometrics\(^4\), and app review commentary supports that finding.

Why not biometrics?

Understanding the opposition’s position regarding biometrics is also helpful to understanding the likely evolution. The two main objections to biometrics are that they too can be hacked and that you can change your password, but you can’t change your biometric. Clearly, no single authentication solution is 100% hacker-proof and if a biometric is hacked, the argument goes, an individual can hardly change their fingerprint or face or eyeball, and so they are at the mercy of hackers for life. This is where encrypted templates, template location and liveness detection apply. This topic deserves its own article, but suffice it to say that these mechanisms safeguard against the theft and manipulation of biometric data.

Another argument against biometrics is that as biometrics are used more frequently, passwords will be more easily forgotten – requiring even more password resets. In addition, passwords continue to serve as the backup mechanism in the event a biometric...
doesn’t work. The issue of stolen credentials doesn’t go away and the backup mechanism could allow a criminal to initiate the password re-set, opening up the possibility for ongoing fraud.

All these are drivers for the coming evolution in biometrics. Although biometrics, like any other authentication option, are not 100% secure from hackers, they are more secure than passwords, and far more convenient. For those reasons, financial services companies will expand their use of biometrics, while they also continue to build out the security ecosystem in which biometrics will play multiple parts.

**Strong customer authentication**

After years of evaluation, banks have determined that biometrics meet their security and usability requirements, and have begun to use the technology for basic consumer app login and call centre verification. Risk in these activities is typically lower, and the primary goal has been to add convenience without sacrificing security. As people increase their use of mobile devices for financial services, however, the level of risk will increase. It will become common for higher-value payments to be made online and via mobile. As these changes occur, banks will use technology to handle risks. The challenge is to do so in a manner that doesn’t impact customer experience – and one answer is step-up authentication – and risk-based authentication.

**“To accommodate increased risk as people carry out more transactions more on mobile, financial institutions will use biometrics as part of a multi-layered authentication solution”**

Risk-based authentication is not new to financial services. For years now, banks including JP Morgan Chase and Bank of the West have allowed users to access basic account information on known devices without any additional authentication. Actual account numbers aren’t revealed in balance checks, and the user can’t take action with the money.

To accommodate the increased risk as people transact more on mobile, financial institutions will use biometrics as part of a multi-layered solution. Some, as mentioned, have already begun using device ID as a simple identifying factor. Many others are using geographic location — thus the need to verify a transaction if you use your card while travelling and haven’t warned your credit card company that you’re going out of town.

Biometrics on mobile becomes another factor of authentication. Furthermore, as passwords are eliminated entirely due to their insecure and unpopular nature, and as biometrics become more commonplace, banks will use multiple biometrics. Initially, they are doing so to enable more of their customer base to access biometrics. Today, fingerprint is only available on devices with a fingerprint scanner, and there are almost no devices available with iris scanners. Many financial institutions are choosing to offer multiple options, including face and eye recognition, to accommodate customers with different devices and different preferences.

“Banks are increasingly using biometrics in their apps to save customers from having to answer security questions when calling a contact centre – security questions are just as unpopular and insecure as passwords”

In the future, financial institutions will offer biometrics for step-up authentication — in fact, this is available now for customers of RSA Security’s Adaptive Authentication mobile SDK product. While there are a few known instances of financial institutions using passwords for step-up authentication, this has proven to be unpopular for reasons already mentioned. Using biometrics for step-up authentication eliminates the friction of passwords.

In addition, financial institutions will offer biometrics as a back-up for passwords. If a user attempts to use a fingerprint and it fails (their skin may be too dry or damp), they can use eye or face recognition as a back-up, eliminating the password vulnerability entirely. Financial institutions will no longer need to maintain databases of passwords that can be hacked, and if they are deploying device-side biometrics, they won’t need to protect databases of biometric templates either.

Financial institutions are keenly aware of the need to balance convenience and risk, but it won’t be their initiative alone that drives changes in authentication practices. Regulatory bodies are getting involved as well. The second European Union Payment Services Directive (PSD2) requires strong customer authentication, and the latest draft Regulatory Technical Standards on Strong Consumer Authentication acknowledges it should be risk-based. And while there isn’t much regulation around authentication in the US, New York recently implemented cyber security requirements for financial services companies, including the stipulation that they use “effective controls, which may include multi-factor authentication or risk-based authentication to protect against unauthorised access” to data.

**Extra uses for biometrics**

Driven by the greater security of biometrics and the expanded use of mobile, financial institutions are exploring other ways for using biometrics. Card-less ATM withdrawals, call centre verification and second-factor or out-of-band authentication for laptop users are three early ways in which banks will use biometrics beyond consumer mobile login. Banks are starting to shift cash withdrawals from traditional ATMs (which are vulnerable to skimmer fraud) to mobile.

---

**BEYOND LOGIN**

Early ways banks will use biometrics beyond consumer mobile login include card-less ATM withdrawals, call centre verification and out-of-band authentication on laptops.
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات