Revival of Biometrics in Banking: Heralding a New Era in mPayments

Banking is now living in an omni channel world. Changing avenues for customers make banking easier, but nevertheless also potentially riskier. The transition of money --- from physical money to e-money -- has also transformed the world of crooks as well; where petty thieves are now capable of committing online fraud.

Forrester Research forecasts that US mobile payment transactions will reach USD 90BN in 2017, registering a 48% compound annual growth rate (CAGR) from the USD 12.8BN spent in 2012\(^1\). Gartner projects that over the next four years the mobile payments industry will experience an average annual growth of 35 percent, creating a market of more than 450 million users worth USD 721 billion by 2017\(^2\). Parallel to this phenomenal growth, the fraud matrix is also growing. There is a common perception that mobile payments platforms are less secure than e-commerce or traditional payment methods.\(^1\) Using 2012 industry market projections on e-commerce sales in North America, CyberSource, a provider of payment processing and risk management services, has estimated that total fraud revenue loss translates to approximately USD3.5 billion\(^3\). Fraud incidents within a span of five years may account for 1.5

---

2. Janessa Rivera and Rob van der Meulen, : Mobile Payment, Worldwide, 2013 Update, Gartner, 4 June 2013
Using 2012 industry market projections on e-commerce sales in North America, CyberSource, a provider of payment processing and risk management services, has estimated that total fraud revenue loss translates to approximately USD3.5 billion.

percent of all mobile transactions, says Avivah Litan, an analyst at technology research company, Gartner.4 The most common threat being that almost 70 percent of mobile phones aren’t protected by passwords5.

Bankers across the world are grappling with ways to find a lever to plug these losses. How can a banker establish the fact that the person transacting is actually a client and not a fraudster? This is where the biometrics science comes into play, and has many bankers excited about its potential. Don Callahan, Citigroup CTO, says, “The idea of biometrics is something that I am excited about. Having digital print is very good. Accessibility to biometrics information is extremely important to us....having an organized back-end process to make sure you are who you say you are, is terrific for the banking industry.”6 Central Banks around the world are also in the process of formulating strategies to mitigate this risk. The Governor of the Central Bank of Nigeria (CBN) is in the process of capturing biometric data of bank customers to ensure better services. Amidst all these happenings, Apple launched the iPhone 5S and, subsequently, Samsung launched its 5S model using fingerprint biometrics for user authentication.

This article aims to bring out the relevance of biometrics technology in the banking world, and suggest why biometrics should be the basis of multi-factor authentication; diagnose fraud prevalent in mobile channels; and, review the effect of new mobile devices being released in the mass market that are embedded with fingerprint technology for mobile payments.

Evolution and Prevalence of Biometrics in Banking

Biometric technologies analyze unique biological traits that differentiate one human being from another, such as fingerprints, the retina or iris or the pattern of an individual’s voice. Data gathered by some of these technologies, particularly iris patterns and fingerprints, are unique enough to distinguish a single individual from the entire global population.

Biometrics in banking has evolved over the years, starting from the 1970s, and has attained some level of maturity. On analyzing various press releases on the Finextra portal, a specific trend is seen emerging. Until 2005, the financial services world used fingerprints, signature recognition, vein pattern, and hand geometry; and after that (post 2005), the technology extended to include Voice Biometrics, Iris Scan, Face recognition, among others.

Hosseini and Mohammadi of Iran, in their analysis of 121 global banks in 2012 had concluded that fingerprints are the most


6 http://economictimes.indiatimes.com/opinion/interviews/weve-changed-banking-the-way-google-changed-search-don-callahan-citigroup-cto/articleshow/16816195.cms
Biometrics in Banking - The Spread

Fingerprint 41%
Hand Vein 7%
Hand Geometry 14%
Fingervein 10%
Iris 5%
Dynamic Signature 4%
Facial 3%
Voice 9%
Keystroke 1%

Employee-Focused 30%
Client-Focused 70%

USA: Biometrics in Action

Client-Focused 22%
Employee-Focused 78%

Surveyed Banks and Their Geography

Americas 39%
APAC 32%
Europe 10%
MENA 19%

Global Banking Survey on Biometrics; N=184
popular biometric technology\(^7\). We have extended this study to include 184 banks with the results being displayed above:

Our study also concludes that fingerprint technology and is used in more than 35 countries. Other important indicators are:

- Customer facing adoptability varies across countries and technology
- Mobile banking related adoptability is rare, with a few banks piloting voice biometrics
- Most of the employee-focused usage is for access to various facilities and applications, including attendance registration

- The USA has the most diverse use of biometrics technology. However, most of USA-based adoption is employee-focused, rather than client-focused, which is in variance with the rest of the world, where the technology is client-focused.

---


---

<table>
<thead>
<tr>
<th>Biometrics Type</th>
<th>Applications Covered</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Signature</td>
<td>Internet banking, Branch banking, Document processing, Workflow automation</td>
<td>Estonia, Israel, USA, China, UK</td>
</tr>
<tr>
<td>Facial</td>
<td>Branch banking, Fraud Recognition, Access control (Data center), Access control (Physical, Treasury), Access control (Building, Time and attendance)</td>
<td>USA, UK, China, Switzerland</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>ATM, POS, ePayments, Access control (Applications), Branch banking, online banking, Fund Transfer, Access control (Physical), Access control (Network), Checking transaction history, Check Cashing, Access control (safe deposit box), Access control (Time &amp; Attendance), Biometric card, Online purchase, Loan Origination, Debit card, Access control(customer information)</td>
<td>Costa Rica, Egypt, Mexico, Singapore, USA, Bangladesh, Benin, Bolivia, Brazil, Brunei, Cambodia, Chile, China, Colombia, Germany, India, Indonesia, Kazakhstan, Kenya, Malaysia, Mauritius, Mexico, Netherland, Nigeria, Pakistan, Panama, Philippines, Puerto Rico, Russia, Saudi Arabia, South Africa, Trinidad, UAE, Uganda, USA, Vietnam</td>
</tr>
<tr>
<td>Fingerprint Plus Iris</td>
<td>Access Control (attendance), Access control (Network, Treasury), ATM, epayments</td>
<td>Oman, India</td>
</tr>
<tr>
<td>Fingerprint Plus Hand Geometry</td>
<td>Access control (Safe deposit), ATM</td>
<td>USA, Japan</td>
</tr>
<tr>
<td>Finger Vein</td>
<td>ATM, Access control (Server room), POS, Branch banking</td>
<td>Poland, USA, Turkey, Japan</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>ATM, Access control (Safe deposit), Access control(Time and attendance)</td>
<td>USA, UAE, Puerto Rico, Saudi Arabia, Ukraine</td>
</tr>
<tr>
<td>Hand Vein</td>
<td>Access control (Data center), ATM, ATM, Branch banking, Access control(Vaults Access)</td>
<td>USA, Turkey, Japan, Switzerland</td>
</tr>
<tr>
<td>Iris</td>
<td>Branch banking, ATM, Internet banking, Access control(Time and Attendance)</td>
<td>Jordan, Yemen, USA, Italy, Turkey, Lebanon, Egypt, Norway, Yemen</td>
</tr>
<tr>
<td>Keystroke</td>
<td>Internet banking</td>
<td>Ecuador, USA</td>
</tr>
<tr>
<td>Voice</td>
<td>Telephone banking, Branch banking, Password/PIN reset, Telephone banking, high-risk transactions, Mobile banking</td>
<td>Australia, Israel, Indonesia, USA, Brazil, Pakistan, China, Netherland, Canada, New Zealand</td>
</tr>
</tbody>
</table>
• Localization of technology: fingerprint and iris in India and Oman; finger vein, hand vein, finger print, hand geometry in Japan; keystroke in Ecuador and USA

• Japanese banks have shown a high level of maturity by offering their customers bank cards with a chip, that carries biometric data

All of the above point to the fact that client-focused biometrics technology in banking is yet to converge globally, and has evolved differently in different geographies. We also observe a correlation between biometric adoption and the flexibility of the core banking system. Emerging market banks were able to leverage client-focused biometrics technology as they run on modern platforms, whereas their counterparts in the developed world could not do so. For example, Capitec Bank of South Africa has been a pioneer in that geography and has been using fingerprint biometrics technology to reach economically less privileged citizens since 2006. It moved on to implement biometric ATMs in 2012.

However, many times, banks have pioneered biometrics in a particular geography and not been able to sustain the momentum. For example, Nationwide, gave up on iris biometrics in 2003 after embarking on the same in 1998. Lack of business benefits and high costs were cited as reasons; e.g., for the ATM project the iris recognition alone was 25 per cent of the cost of the ATM, meaning it would not be cost-effective for a wider rollout.

Our study also concludes that fingerprint continues to be the most popular technology and is used in more than 35 countries.

It is a strategic imperative to fall back on the multi-factor authentication with biometrics at the front. It is all about combining the facts of “what you have”, “what you know” and “what you are”.

It may also be noted that many cases included in our study take into account POC stage implementations, and there was no follow-up information available. A few IT solution providers have tied up with third parties and white-labelled biometrics products for employee-focused applications. However, the focus must
soon shift to client-focused applications such as channels.

Future growth of biometrics mooted around multi factor authentication

The banking world has seen the prevalence of two-factor authentication for some time now; but fraudulent transactions are growing year-on-year. When we transact virtually, our identities are determined by IP addresses, various “keys” and passwords, most of which are susceptible to tampering and fraud. Therefore, it is a strategic imperative to fall back on the multi-factor authentication with biometrics at the front. It is all about combining the facts of “what you have”, “what you know” and “what you are”. To carry out a mobile payment transaction, you may have the mobile device and know the transaction pin, but if you are not authenticated by personal traits, such as fingerprint, you may not be able to access the device to complete the transaction.

While we encounter technology sophistication in what we have and what we know, we still are far from achieving industry best practices on what you are, i.e. biometrics, across channels.

We now have an ISO standard 19092:2008 related to biometrics security framework in the financial industry. It clearly establishes the security requirements for the implementation and management of state-of-the-art biometric identification technology. As per the framework, the enrolment repository is connected to a management console that helps configure biometric parameters for enrolment, authenticates users and allows system access privileges. DB Research also states that biometric authentication methods enjoy a remarkable degree of acceptance among the European population. Hence, there is a growing probability that biometric technologies could also be applied in banking.

Changing Channel Priorities: Growth of Mobile Banking and Challenges

In an omni channel world, banks need to adopt a “bricks, clicks and touch” strategy, revolving around the concept of security, accessibility, personalization and convenience. Achieving this is a Herculean task amid changing customer channel adoption trends. Taking the trends from the CEB TowerGroup Report titled “Planning Your Cross-Channel Future” published in December 2012; mobile banking transactions in the USA are projected to grow by 240% between 2010 and 2015. In the same period, online transactions are expected to grow at 10%, ATM transactions by 7.3%, whereas the contact center and the branch are expected to see a decline in transactions.

This changing channel priority has put additional pressure on banks. Banks are not equipped to handle the fraud instances related to mobile banking. Access control is the first level of security and this has generally been managed well through two-factor authentication of Password, OTP/PIN in an online channel scenario, but in the case of mobile banking, the threats are not clear. Each passing day, new malware are being identified, and many devices
are not password protected. As per the Third Annual Mobile Threats Report, mobile malware has grown by 614% from March 2012 to March 2013 and 73% of all malware exploit holes in mobile payments by sending fraudulent premium SMS messages, each generating around 10 USD in immediate profit. The technology platforms, iOS, Android, Symbian, BlackBerry, Java ME have varied threat indications. The most disturbing fact is that the popular platforms are threat prone. The Internet Security Threat Report 2014 reported that 97% of malicious threats by platform is reported for the Android platform. However, it was intriguing to note that 102 (82%) documented mobile vulnerabilities by platform for 2013 was recorded for the iOS platform. The threat is increased when access is not secured, and if a device is used to access unwanted content, there is a greater possibility of malware infesting the system.

A paradigm shift in Mobile Payments: Fingerprint biometrics securing access control

The launch of the iPhone and the iPad are highly disruptive trends in banking. With the launch of iPhone 5S and Samsung 5S with a fingerprint scanner, embedded within the phone's hardware, the world of biometrics will open up, especially in mobile payments. Internally, Apple allows biometrics-authentication for iTunes, and this has a huge potential for the future of payments. The availability of biometrics authentication at the source is certainly a giant change in the banking world.

A few instances reported during 2013 and early 2014 suggest that fingerprint biometrics is gaining mainstream acceptance:

- iPhone 5S, launched with fingerprint sensor that allows users to unlock their phone with their fingerprint, and verify purchases on iTunes without having to input a password
- Samsung 5S, launched with a fingerprint scanner
- HTC has launched One Max with 5.9-inch display and fingerprint scanner
- Fujitsu Disney-branded F-07E Android device, launched with fingerprint sensors
- Motorola, working on phone with fingerprint sensor
- Microsoft Windows 8.1, offering enhanced support for fingerprint sensors
- Diebold has launched a new line of fingerprint ATMs in Kenya
- The Indian government has given a go-ahead for fingerprint or eye scan enabled ATMs to leverage the biometric-based Aadhaar number, which establishes uniqueness of every individual on the basis of demographic and biometric information
- Biometric ATMs are being filed for a new patent application by Bank of America. This patent application outlines a system for authenticating users with a combination of a pin-code and fingerprint biometrics

Mobile devices with biometrics will help provide the first level of security, which Symantec calls traditional access control. If the voice biometrics based pilot being carried out by ING Direct Canada and ANZ is successful and the Bank of America patent for authenticating mobile transactions through voice biometrics gains mainstream acceptance, we may soon see biometrics playing a role in replacing OTP/Pins.

This development may be termed disruptive, not because mobile-based payments may potentially get safer, but also because this change must be looked from a liability perspective. The fraud liability at self-service channels lies with the clients. In the biometrics scheme of things the customer has to be present...
in person, while making a transaction. And, in this context, customers are safer if biometrics evolve to the core of the mobile payment scheme of things. Customers are an important part of the mPayments value chain and the recent wave of fingerprint biometrics being circulated in the mass market embedded within the phones will, in all possibility, trim down the fraud matrix.

The Biometric Research Group expects that worldwide mobile payment transactions will reach USD 250 BN in 2014, reaching USD 750 BN in annual transactions with more than 700 million users by 202013. Biometrics will accelerate mobile commerce, especially in North America, because the technology can offer a higher level of security, while providing an intuitive customer experience. It also expects that over 90 million smartphones with biometric technology will be shipped in 2014. The Group predicts that Apple will initially lead in the deployment of such devices, due to fact that the firm is the first consumer electronics provider to introduce biometric technology to the global smartphone mass market.

Conclusion

The detrimental factors in the growth of biometrics have been higher cost, ambiguity related to standards, and the proliferation of diverse technologies. It was also a bank-led activity, where banks had to invest in costly biometrics technology. The world needs simplicity and ubiquity for a technology to succeed. And, probably we are in one such watershed moment, where biometric standards are in place, and where mobile devices with fingerprint biometrics technology can shift the cost burden from bankers to the consumer. Fingerprint biometrics seems to be the new buzzword that will bring in disruption in the mobile banking transactions space.

We must, however, remain cautious, as we have seen the failure of Motorola’s Atrix Smartphone with fingerprint reading technology due to its inconvenient position at the back of the phone and its slow processing. The current phase must be seen as a resurrection, where biometrics technology is poised to occupy a central position in fraud prevention.

It assures the convenience of use and delivers the prospect of fraud prevention at the customer end — a secure first level access point to facilitate safe and seamless mobile transactions. While a few analysts still remain sceptical about the role of biometrics in future fraud-prevention capabilities, it looks like banking consumers are gradually embracing it. A survey commissioned by ANZ showed that 79 percent of Australians said that they are comfortable with fingerprint technology replacing banking PINs.14 We may soon be seeing a safer world of mobile banking, heralding a new era in mPayments.
