



# Biometrics in the Payments Space

*Financial institutions advised to monitor authentication innovation*

**By Nicole Reyes**

TMG Senior Fraud Prevention Analyst

**bi-o-met-rics**  
(bīō'metriks) *n.*  
*the identification of humans by their characteristics or traits, used as a form of identification and access control*

In fall 2013, Apple impressed the mainstream consumer world by equipping the iPhone 5s with fingerprint identification. One year later, the company rolled its biometric solution into its mobile wallet, Apple Pay, which relies on a three-prong approach to security with fingerprint ID, near-field communication (NFC) and tokenization. For financial institution (FI) leaders charged with innovating to meet changing consumer expectations, authentication methods will be an important area on which to keep a bead. The iPhone's fingerprint scanning technology provides a good test of the market.

Leading-edge consumers will become increasingly important for FIs, as many of them represent the future of banked consumers.

Are consumers ready for biometrics? In a recent survey, nearly half of respondents indicated comfort with biometrics, such as fingerprint, palm or iris scanners, as authentication methods.<sup>1</sup>

Indeed, many iPhone users have welcomed the innovation, largely because it has made life just a little bit easier for them. While those of us in the security profession would like to think it was the increased safekeeping of their personal data and information that intrigued iPhone fans, we know most people are just as excited about speed and simplicity as they are about security. A recent survey, for example, found only 28 percent of respondents are very concerned with the privacy and security of their phones or mobile devices.<sup>2</sup>

An alternative to the iPhone's traditional PIN access, "Touch ID" enables fingerprint scanning with a microscopic camera capable of capturing and comparing high-resolution images to saved profiles. Unlike other fingerprint-scanning devices, the iPhone 5s identifies the fingertip print, which is more difficult to lift and fake as a means for unauthorized entry into a device.

There are also those early adopters who are attracted to anything new or interesting, simply because it's new and interesting. These are the individuals with the influence to take an innovation from cult trend to mainstream market position. They are the leading-edge consumers who will become increasingly important for FIs, as many of them represent the future of banked consumers.

### **Are Consumers Ready for Biometrics?**

Biometric technology may be burdened by a bit of a "creepy" factor, as consumers worry about organizations storing and sharing their most personal and private information, namely the makeup of their bodies. The same survey that polled consumers about the iPhone asked about this concern, and 51 percent said they would be worried about giving a mobile device or company access to their fingerprints.

Of course, it's one thing to check a box on a survey; it's quite another to resist the siren call of ease and convenience. Consumers all over the world are demonstrating comfort with sharing their personal and account information with a variety of parties. Take Disney park visitors, for example, who wear RFID bracelets for days on end. These bracelets act as park tickets, attraction passes, room keys – and even as credit cards. They also allow Disney (and potentially the third parties it does business with) to track their customers' every move and transaction while visiting.<sup>3</sup>

1. "Biometric payments trump social, smartphone and contactless tech for security-conscious shoppers," WorldPay, June 13, 2013

2. "iPhone Fingerprint Survey: Over Half Interested in New Feature," AYTM, September 18, 2013

3. "At Disney Parks, a Bracelet Meant to Build Loyalty (and Sales)," The New York Times, January 7, 2013

Biometrics not only provides an elevated level of security; the technology has been proven to work across a variety of platforms and devices.

Guests are also able to use their Disney RFID bracelets to stay up-to-date on their account balance throughout their Disney experience. This convenience from a multi-purpose, smart device is ideal for consumers looking to speed up transactions – whether that’s passing through a turnstile or buying a pair of mouse ears.

### Biometrics Across Platforms

Fraud is an ever-present, increasing concern in the world of payments, and the desktop computer is far from the only digital gateway available to cunning fraudsters. Relentless and resourceful cyber criminals make it necessary for consumers – and the FIs who protect them – to participate in the improvement and development of security measures. This requires innovation and diligence over a multitude of platforms and devices; as the consumer has gone mobile, so too have fraud attempts. In 2011, more than 60 percent of mobile device users were not using a PIN to secure access. As more sensitive information is transmitted via mobile devices, consumers and FIs must find secure ways to handle personally identifiable information and financial transactions no matter where they originate.<sup>4</sup>

Enter biometrics, which not only provides an elevated level of security; the technology has been proven to work across a variety of platforms and devices. This is important as more consumers rely on several types of convenient tools to work, live and play.

Biometric security is still an infant in the financial world, so its proponents are working hard to prove its importance, relevancy and ability to move the needle in the fight to mitigate fraud losses. These supporters will tell you that biometric security is the way of the future, namely because of its absolute reliance on the presence of the individual. Fraudsters simply cannot enter secure devices or accounts without the necessary biometric profile. Of course, reliance on the presence of a biometric profile can, in some circumstances, lead to other types of criminal activity among those hoping to gain access to secure systems.<sup>5</sup>

### Biometrics for Payment and Other Transactions

Biometric technology, such as fingerprint scanning, is not a new method for entry into secure systems; we have seen this technology on several different laptop brands, for instance. Many of these machines are equipped with the hardware and software that enable fingerprint scans for online password authorization.

Apple has taken that existing technology and introduced it to the mainstream smartphone user via the iPhone. The company’s Touch ID began with the iPhone 5s and has since taken on a more critical role in the iPhone 6 and 6 Plus

4. "Mobile Tech Security and Biometrics Sector Stock Snapshot: AAPL, NXTD," SmallCapNetwork.com, September 16, 2013

5. "Malaysia car thieves steal finger," BBC News, March 31, 2005

with its inclusion in payment authentication. However, biometrics plays a role in more than just Apple's mobile wallet solution. In addition to Apple Pay, other Apple applications, such as the App Store, iBooks Store and iTunes Store, can also verify payment transactions with fingerprint profiles.<sup>6</sup>

Fingerprint scanning is not the only biometric method potentially headed for payment authorization. Other types of biometric capabilities, such as facial recognition, for example, have already permeated society in numerous ways – from security cameras charged with identifying cheating gamblers to social media sites that encourage users to identify friends in photos. It's not a stretch to consider facial recognition in payment scenarios. In fact, a Finnish company, Uniqul, has patented and tested a payment system that lets consumers pay their bills and make purchases with only their faces.<sup>7</sup>

Some corners of the payments space are also turning to biometric security as another tool for mitigating ongoing and increasing fraud trends.

The ATM is one channel in particular that is faced with rampant fraud and in need of new technology to thwart criminals from attacking the often isolated machines. In Japan, ATMs have been equipped with vein-profile scanning in response to the country's high rate of ATM fraud. As light is emitted from the scanning device, an image of the vein placement in a cardholder's hand is captured and compared to the stored profile on his or her bank card. As with the iPhone, the biometric profile is stored on an internal computer chip, rather than in a distant computer database.<sup>8</sup>

NXT-ID, Inc., is a U.S. company that is leveraging the growing mobile commerce market for its development of biometric security software. Launched in August 2013, the company's FaceMatch product utilizes cameras already present in mobile devices to recognize and identify users for access to the device and for authorization of secure transactions, which may someday include payments. As well, the company is working to push out its own digital wallet solution that is both passcode- and voice-protected.<sup>9</sup>

### The Future of Biometrics

Techies and industry experts alike say biometrics in the payments space will not be a passing fad. Rather, they insist the authentication method will be a long-term and solid addition to all transactional industries. With the entry of more biometric-enabled products into the mainstream marketplace, consumers are naturally taking notice. As with any technology innovation, however, developers must prove the tool is not only valuable, but simple. In other words, consumers may like the idea of security, but they love the idea of simple.

Consumers may like  
the idea of security,  
but they love the  
idea of simple.

6. "iPhone 5s Fingerprint Scanner: 9 Security Facts," InformationWeek.com, September 11, 2013

7. "Finnish Company Develops Facial Recognition Payment System," Mashable, July 25, 2013

8. "The Biometric Wallet," IEEE Spectrum, May 30, 2012

9. "NXT-ID Expects to Profit from Digital Wallet," Paymenteye.com, September 30, 2014

Processors, acquirers, merchants and FIs that are right now staring down the country's adoption of EMV and tokenization may do well to also monitor the development of biometric security solutions. An increase in the development of biometric security on mobile devices can only mean dramatic change for mobile commerce. As we've seen in the last 10 years alone, futuristic – and sometimes even far-fetched – solutions are finding their way into the mainstream with increased speed, and often without the help or even support of traditional financial industry players.

Whether they are ready or not, whether they understand it or not, many early-adopter consumers will be intrigued by the promise of biometric security solutions. For FIs, the question becomes: Will our customers lead us or will we lead our customers?

---

#### ABOUT THE AUTHOR



**Nicole Reyes** is a Senior Fraud Prevention Analyst for The Members Group (TMG). In this role, Nicole researches and analyzes current fraud trends and actively manages the fraud-prevention strategies for TMG's financial institution clients. She is also an important part of TMG's fraud detection and prevention product implementation team. Nicole's passion is to help credit unions and community banks mitigate their fraud losses by utilizing proactive and innovative methods. Nicole has been with TMG since 2007 and has more than 13 years of card industry experience. She can be reached at [nicoler@themembersgroup.com](mailto:nicoler@themembersgroup.com).

---