



## Alive And Starting To Kick

*Jim Daly*

**As they rapidly evolve, biometric technologies are certain to play a greater role in payment authentication. But, given consumer acceptance and other issues, just how big this role will be is up for debate.**

**W**ith most new developments in payments, there's a whole lot of talk before any discernible action. Take biometrics. Backers of this diverse family of technologies say using credentials derived from a consumer's fingerprints, face, eye, or other physical attributes offers a far superior way of authenticating a purchaser than easily compromised user names and passwords.

Talk about biometrics in payments goes back at least a dozen years. A startup called Pay By Touch put biometrics on the map with its fingerprint-identification technology. But over-expansion and management blunders caused Pay By Touch to implode in 2008.

Since then, biometric systems, especially those for online and mobile payments, have multiplied faster than cells in a zygote. But such systems are still much more the exception than the rule in payment authentication.

While many observers agree that biometric technology works, questions about consumer acceptance, reliability, and other issues are sources of heated debate. And while quite rare, data compromises involving biometrics can happen, potentially creating nightmares for affected consumers.

Perhaps the biggest impediment to wider adoption of biometrics comes down to pure convenience. For most consumers, it's still easier to default to entering a password. Across all age groups—even tech-savvy Millennials—the familiar user ID/password combo is rated as the easiest identification method to use (chart, page 25).

### ***'We Have a Problem'***

Despite the security shortcomings of user names and passwords, biometric systems that would replace them impose hassles such as requiring scans of whatever body part is to be recorded. Sometimes they aren't as easy to use or as reliable in a point-of-sale or online purchase as the older technology.

"We have a problem right now with biometrics in that the convenience isn't as high as it could be," says Tim Sloane, vice president of innovations and director of the Emerging Technologies Advisory Service at Maynard, Mass.-based Mercator Advisory Group Inc.

A chorus of "we're working on that" summarizes how biometrics promoters are responding to that issue. It seems everyone these days, from

the payment card networks to processors to mobile-phone manufacturers to tech startups, have biometric projects in the works.

At the same time, biometrics is beginning to move beyond pure physical attributes—hand, face, and iris scans, for example—to include data derived from the way a person behaves, especially in relation to computers and mobile devices.

This technology, called behavioral biometrics, can track the speed and force with which a person uses a desktop computer's keyboard, or the way a person holds and uses a smart phone, among many variables.

"There's hundreds and hundreds of data points you can collect," Ryan Wilk, vice president of customer success at Vancouver, British Columbia-based biometrics developer NuData Security Inc., said in late May during a panel session at the CNP Expo, a conference in Orlando, Fla., about online and mobile commerce.

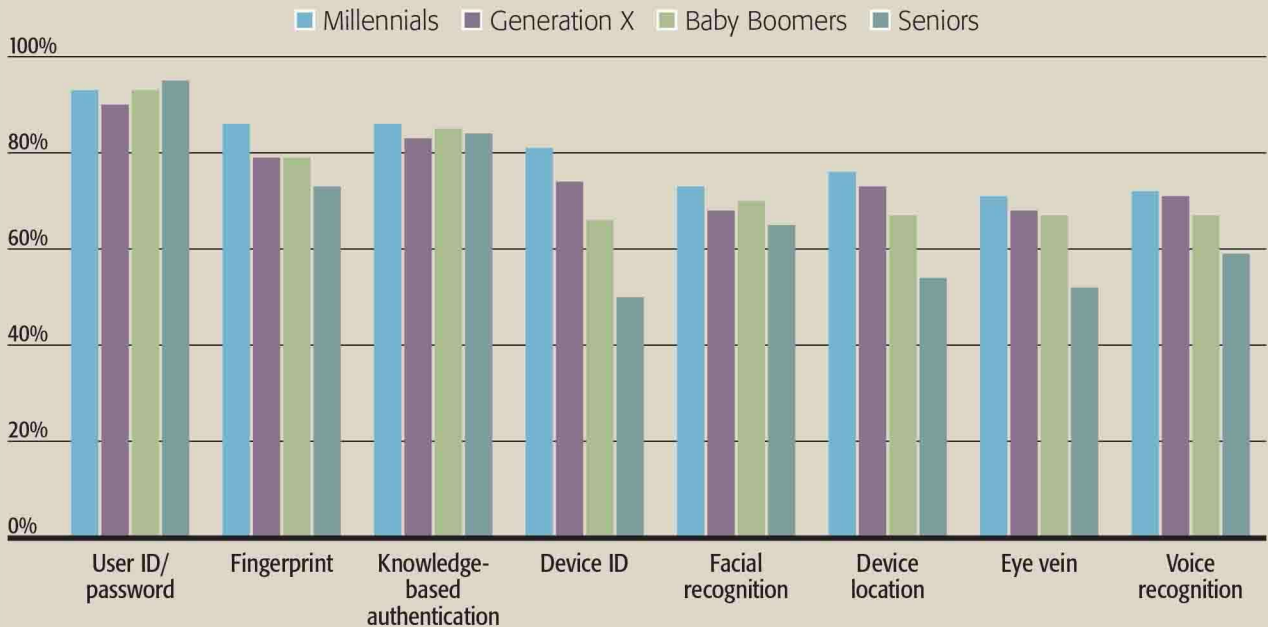
### ***Line of Defense***

Biometrics took center stage in 2014 when Apple Inc. unveiled the Apple Pay service for its iPhone. The service can record one or more of the iPhone owner's fingerprints, then use that print to authenticate an Apple Pay purchase.

Similarly, the rival mobile-payments service Android Pay from Alphabet Inc.'s Google unit supports

# For Ease of Use, Consumers Give User IDs and Passwords Top Marks

(Percent of respondents rating identification method as easy or somewhat easy to use)



Note: Respondents asked to rate the methods as very easy, somewhat easy, somewhat difficult or very difficult to use, or don't know.  
 Source: Aite Group LLC research via Federal Reserve Bank of Atlanta, January 2017

fingerprint-authenticated payments on phones using the Android operating system that have fingerprint sensors. And device manufacturer Samsung's Samsung Pay supports both fingerprint and iris scans.

Still, the "Pays" have had their share of problems with biometrics, according to Mercator's Sloane. If the phone's sensor can't read a fingerprint, the consumer can't authenticate herself to the mobile wallet. And beyond biometrics, there remains

the entire issue of lack of merchant acceptance of the mobile wallets.

None of that has stopped experimentation with new biometric systems. The thinking among many payment executives is that, rather than a cure-all for fraud, biometrics can best be used as one more line of defense for protecting the consumer's identity and ensuring authentication of legitimate transactions.

"It's all about layers of security," says Dennis Gamiello, vice

president of identity solutions at Mastercard Inc. "The real value is when it [biometrics] is combined with other elements."

In contrast to the assumption that a person who, to the merchant, looks like the person who recorded his picture in a mobile wallet and therefore should be approved no questions asked, biometric authentication typically involves a probability-based score.

Behind the scenes, the technologies compare the stored biometric with the one presented for authentication. "They're probabilistic," says Gamiello. With a high enough score, "we can be really sure it's you."

Mastercard found itself in the biometrics spotlight a couple of years ago when it unveiled Identity Check Mobile, a mobile-based service using facial-recognition technology. Media outlets quickly dubbed it "Selfie Pay," and suddenly biometrics was all over the news. Mastercard tested

'It's all about layers of security. The real value is when [biometrics are] combined with other elements.'



the system in Europe and Canada beginning in late 2015 and last October launched it with BMO Bank of Montreal on the bank's commercial cards. The service also employs fingerprint technology.

Now Mastercard is working with partner issuers in more regions, including the U.S., to bring an updated Identity Check Mobile to the issuers'

customer identity in bank branches when identification is required, such as when applying for a loan.

The system replaces the typical process in which tellers or other bank personnel would look at a customer's driver's license, then do manual lookups or review other databases for further confirmation, according to Chris Van Der Stad, senior vice

About 50 financial institutions are now using Verifast for customer or employee identification. And Fiserv is working with some ATM manufacturers to bring the technology to interactive teller machines, the high-end ATMs that offer video communication between the customer and a centrally located teller.

### 'Kind of Creepy'

Fiserv has tested any number of biometric technologies, including facial, retinal, and voice recognition. The company not only wanted to find out how the technologies worked, but also consumers' reactions to them.

"Interestingly, the eye recognition did not test very well at all, people found it kind of creepy," says Scott Hess, Fiserv's vice president of user experience consulting and innovation. "Technically, they all worked very well."

Besides more development in the pure biologically based authentication systems, new services based on behavioral characteristics are getting attention from payments firms.

With little fanfare, behavioral biometrics began appearing on the radar screens of payment card security executives about two years ago. Now, experts predict that behavioral biometrics will assume a more prominent role in protecting transactions



Mastercard's Dennis Gamiello using the facial-recognition feature of the company's Identity Check service.

(Photo: Mastercard Inc.)

mobile-banking apps, according to Gamiello. Distribution through financial institutions' apps is "the way to scale this product," he says.

Other material in Mastercard's biometric test tube includes a fingerprint-reading sensor on an EMV chip card. The card draws on the point-of-sale terminal's power source, foregoing the need for a battery.


Once inserted in the terminal, the card's sensor compares the stored thumbprint with the thumbprint of the person at checkout. If they match, you've got a sale. Currently under test with a bank in South Africa, the card is set for rollout later this year. Mastercard plans to bring it to other regions, according to Gamiello.

"It's really meant to be a low-touch, low-investment card," he says.

As demonstrated by the "Pays" and Mastercard's South African test, fingerprints—and hands—are popular foundations for biometric authentication. Financial-institution processor Fiserv Inc. in June 2016 introduced its Verifast: Palm Authentication technology to confirm

president and chief technology officer, Open Solutions, at Brookfield, Wis.-based Fiserv.

With Verifast, the teller enrolls the customer by having him hold his hand over a small countertop device for about 15 seconds in order to gather 5 million data points from the palm. The data are then encrypted and available for future authentication. The basic technology comes



"Unlike a physical biometric or a user name and password, it's very difficult to take your passive biometric, to take your natural interaction, and attempt to spoof."

—RYAN WILK, VICE PRESIDENT OF CUSTOMER SUCCESS, NUDATA SECURITY INC.

from Japanese tech giant Fujitsu, and it runs on Fiserv's DNA account-processing platform.

"The problem we were trying to solve was the in-branch experience of consumers," says Van Der Stad. "We wanted to dramatically improve that."

as e-commerce and mobile commerce continue gaining share of retail sales and the Internet of Things makes payments possible from billions of devices.

Sometimes called passive biometrics, behavioral biometrics tracks

patterns in the way a person moves, behaves, or uses something physically. Handwriting, gait, and other physical motions “all can be measured,” David Lott, payments risk expert at the Federal Reserve Bank of Atlanta, said at the CNP Expo panel session he moderated.

NuData’s technology creates a user profile that “is very difficult to spoof, very difficult to attempt to steal,” Wilk said. “That’s the beauty of passive biometrics—that unlike a physical biometric or a user name and password, something that someone else can take from you, it’s very difficult to take your passive biometric, to take your natural interaction, and attempt to spoof.”

Mastercard saw enough potential in NuData’s technology that in late March it announced an agreement to buy the firm for an undisclosed price. NuData’s flagship NuDetect product separates legitimate users from potential fraudsters based on their online, mobile-app, and smart-phone interactions, and flags high-risk behavior.


The technology assesses, scores, and learns from each online or mobile transaction to enable merchants and card issuers to make near real-time authorization decisions, Mastercard said.

on their capabilities, cost, and operational issues, as well as the particular needs of the merchant, bank, or other entity using them.

“There is no single authentication modality that’s bulletproof, and there is no single modality choice that’s the best choice in all cases,” said Lott.

### ‘Software Savants’

As adoption increases, biometrics also poses questions about consumer privacy. Privacy rules are stricter in Europe than in the United States,



‘Using behavioral biometrics, and using some traditional biometrics such as face and voice, your phone is always checking who you are.’  
—TIM SLOANE, VICE PRESIDENT OF INNOVATIONS AND DIRECTOR OF THE EMERGING TECHNOLOGIES ADVISORY SERVICE, MERCATOR ADVISORY GROUP INC.

where panelists said they believe regulators will stay out of the way if merchants and financial institutions confine their usage to fraud and risk control. Problems could arise if companies use biometrics for consumer tracking and marketing purposes.

“Then it hurts the entire industry,”

concept he calls “persistent identity,” which is essentially a variant of behavioral biometrics.

Persistent identity would be built on the many metrics a consumer’s smart phone can capture, including geolocation, and work and commuting patterns. Under such a system, a so-called challenge event that would require presentation of a biometric such as voice or facial recognition would be reserved for high-risk transactions.

“Using behavioral biometrics, and using some traditional ... biometrics

such as face and voice, your phone is always checking who you are,” says Sloane.

Sloane’s concept delves into the realm of artificial intelligence and so-called machine learning, terms that are much used in tech circles these days but are rather ill-defined. Computers are still incapable of thinking like humans, Sloane notes, but continual advances in machine learning are laying the groundwork for new applications, what he calls “software savants.” These “savants” can do very specialized tasks, such as looking for fraudulent payment transactions in a vast data pool, very well.

“A savant has what machine learning can do—exceed human capabilities in a very narrow domain,” says Sloane.

While they’re not as fast as machines, look for humans to greatly boost their learning about biometrics in the coming few years, particularly as the need for greater payment security increases, and technological development builds upon development. **DT**



While Mastercard’s acquisition of NuData may signal that behavioral biometrics are gaining traction, other panelists at the CNP Expo session pointed out that the many forms of biometrics all have their strengths and weaknesses. Their usage depends

said panelist Bernard McManus, head of global fraud management and strategy for Sony PlayStation.

Mercator’s Sloane believes the hassles of PIN entry, as well as current biometric systems, some day could be reduced through a