

BIOMETRICS IN THE PAYMENTS INDUSTRY

WHY BIOLOGICALLY BASED AUTHENTICATION IS BECOMING THE GO-TO SECURITY FEATURE FOR ENABLING DIGITAL COMMERCE

July 2016

Jaime Toplin | Research Associate

KEY POINTS

- **US smartphone makers are rapidly integrating biometrics-based features, such as fingerprint scanners, into their devices.** BI Intelligence forecasts that 99% of installed smartphones in the US will be equipped with fingerprint scanners by 2021. The shift will happen much sooner for the installed base of iPhones in the US — nearly all of which will be biometrics-enabled by 2018.
- **The global biometrics industry is becoming lucrative.** Global mobile biometrics market revenue, including sensor revenue from mobile devices, fees and revenues from biometric app downloads, and authentication-fee revenue from payment transactions, will reach \$34.6 billion in 2020, according to Acuity Market Intelligence.
- **Biometric verification is valuable to payments and commerce firms because it keeps data secure without inconvenience to consumers.** Passwords and PINs aren't good security mechanisms — they're arduous to input and hard to remember, particularly on the small screens of mobile devices. Biometric verification is a more secure solution for apps and devices that also bypasses the need to remember a password.
- **Fingerprints can already be used to unlock phones, verify mobile wallet payments, and open access to banking apps, among other applications.** As of January 2016, 608 financial institutions in the US offered fingerprint authentication in their mobile banking apps, up from just 252 in October 2015, according to research firm Celent.
- **Biometric technology is moving beyond fingerprints.** Right now, biometric verification is largely concentrated on fingerprint-scanning technology on mobile phones. But the technology is expanding, and other verification methods, including facial recognition and iris scanning, are becoming more popular.
- **Biometrics do pose their own security challenges.** The unique nature of biometric verification, and the fact that the digitized record is stored locally in a secure portion of the phone, makes this data far more protected than traditional verification methods. But the risk to this type of data is also greater because unique, permanent biological identifiers are very valuable to hackers.

[Download the charts and data in Excel »](#)

INTRODUCTION

Rising digital fraud, growing concern about data privacy, and difficulty remembering an endless stream of letters, numbers, and characters, are rendering traditional mechanisms for verifying one's identity online, like passwords or PINs, ineffective. So firms have begun to explore additional pathways for verification — in particular, biometrics has emerged as one of the top alternative authentication technologies.

Biometrics are unique biological measurements that can be digitized and turned into a trackable record, according to [Find Biometrics](#). These measurements, which include but aren't limited to fingerprints, facial and vocal patterns, and vein profiles, have long been used by law enforcement to verify identity. But now, as individuals lean more heavily on digital technology, such identifiers are being adapted for the consumer technology space. Biometrics can be used to verify consumer identity, while limiting access to, and protecting, sensitive consumer information.

Major smartphone vendors including Apple, Samsung, and HTC have added biometrics features to their phones in the past few years. In turn, app developers are looking to incorporate biometric security into both payments- and nonpayments-related applications — and this is leading to a rapidly growing market for biometrics and relatively speedy consumer adoption.

In this report, we size the phone-based biometrics market in the US, explore why payments and commerce firms are rapidly integrating biometrics-based authentication into their processes, and examine the factors that could affect integration and adoption.

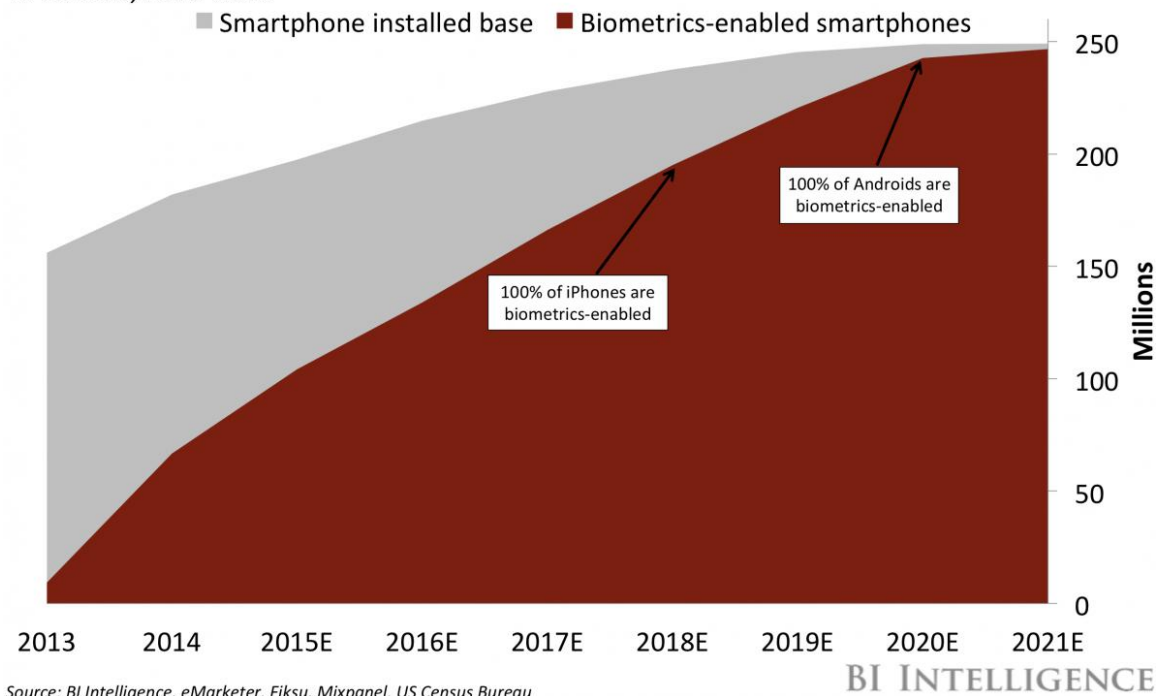
THE BIOMETRICS MARKET

The number of smartphones that are biometrics-enabled in the US has risen rapidly since Apple introduced the first iPhone 5S in late 2013. We estimate that 62% of the installed base of smartphones will be biometrics-enabled by the end of 2016. BI Intelligence forecasts that by 2021 nearly all smartphones in the US will integrate biometrics.

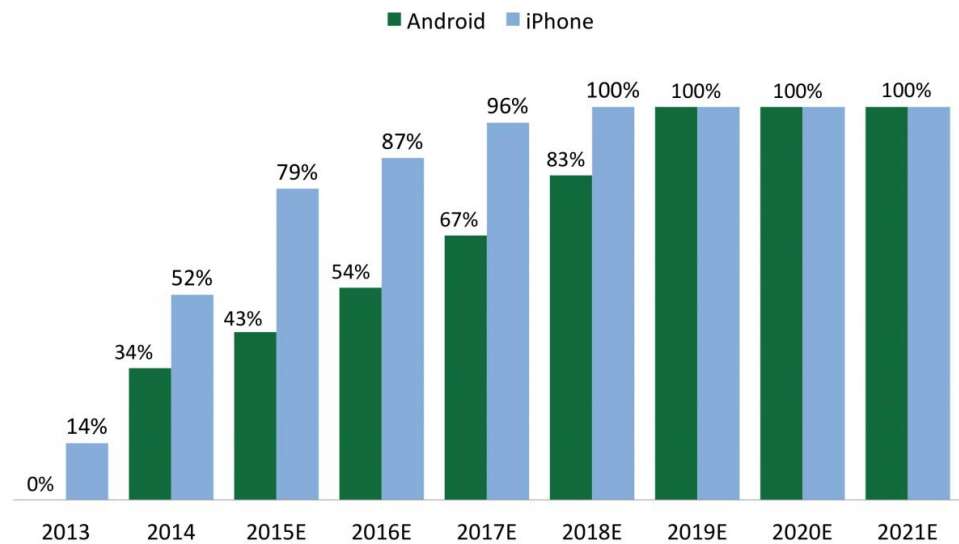
That equates to roughly 247 million biometrics-enabled smartphones in 2021, a significant jump from just under 10 million in 2013 and almost double the estimated 132 million for 2016. The shift will happen much sooner for the installed base of iPhones in the US — nearly all of which will be biometric-enabled by 2018 — than for Android phones, which should reach 100% penetration by 2020.

FORECAST: Biometrics-Enabled Share Of US Smartphone Installed Base

In millions, 2013-2021



FORECAST: Percentage Of Biometrics-Enabled US Smartphone Installed Base, By Operating System 2013-2021



Source: Fiksu, Mixpanel

BI INTELLIGENCE

There are a few important things to note about this forecast, which is based on data from [BI Intelligence](#), [eMarketer](#), [Fiksu](#), [Mixpanel](#), and the [US Census Bureau](#):

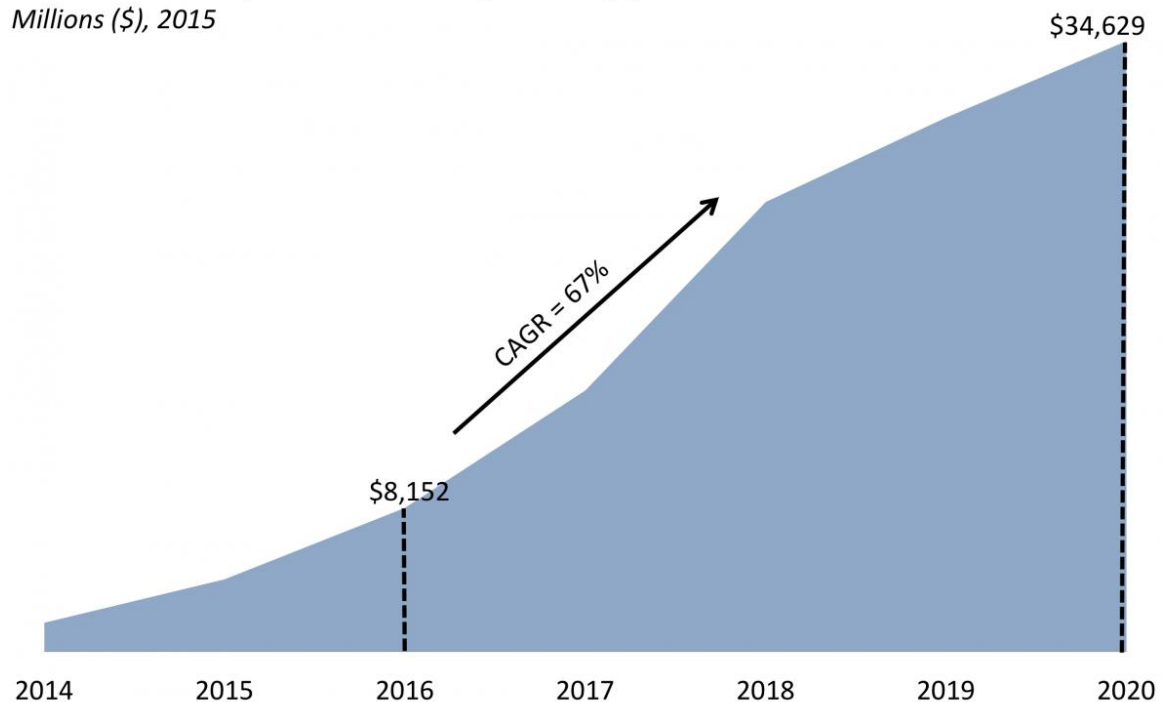
- **More smartphone users:** Roughly 60% of the US population owned a smartphone in 2015, and that will increase to roughly 71% by 2021 as mobile phones become the primary computing device.
- **Slower overall growth:** Given the typical tech adoption curve, the pace of growth for biometrics-enabled smartphones will slow somewhat from the rapid penetration of the past few years. In addition, the mobile phone upgrade cycle is expected to lengthen as users forgo contracts and hold on to their phones for longer. Eventually, though, almost all smartphone users will be pushed to upgrade as nonbiometric-enabled phones become too old to run the latest operating systems or apps.
- **Faster growth for Android phones:** For Android devices, which became biometrics-capable later than iPhones, penetration rates will increase rapidly over the next few years. This forecast uses data on Samsung phones to represent the US Android market, as Samsung phones dominate that market and illustrate its likely trajectory. Samsung introduced biometrics-enabled devices in early 2014, about seven months after Apple did. Other device makers, which hold a considerably smaller share of the market, started adding such functionality in 2015 and 2016.

Fingerprint scanners were one of the first biometrics features introduced for security purposes and are now widely used to unlock devices: 89% of iPhone users with Touch ID enabled are using the feature, according to [Techpinions](#). Now, as more phones become biometrics-enabled, biometrics will be integrated into apps and platforms. With such strong usage, app developers have a compelling reason to implement the feature where added security is important, like mobile wallets, apps, and on digital transactions.

Biometrics are becoming a lucrative global industry. Global mobile biometrics market revenue, including sensor revenue from mobile devices, fees and revenues from biometric app downloads, and authentication-fee revenue from payment transactions, will grow at a 67% seven-year compound annual growth rate (CAGR) to reach \$34.6 billion in 2020, up from \$1.62 billion in 2014, according to [Acuity Market Intelligence](#).

Annual Mobile Biometric Revenue From Devices, Transactions, And Apps

Millions (\$), 2015



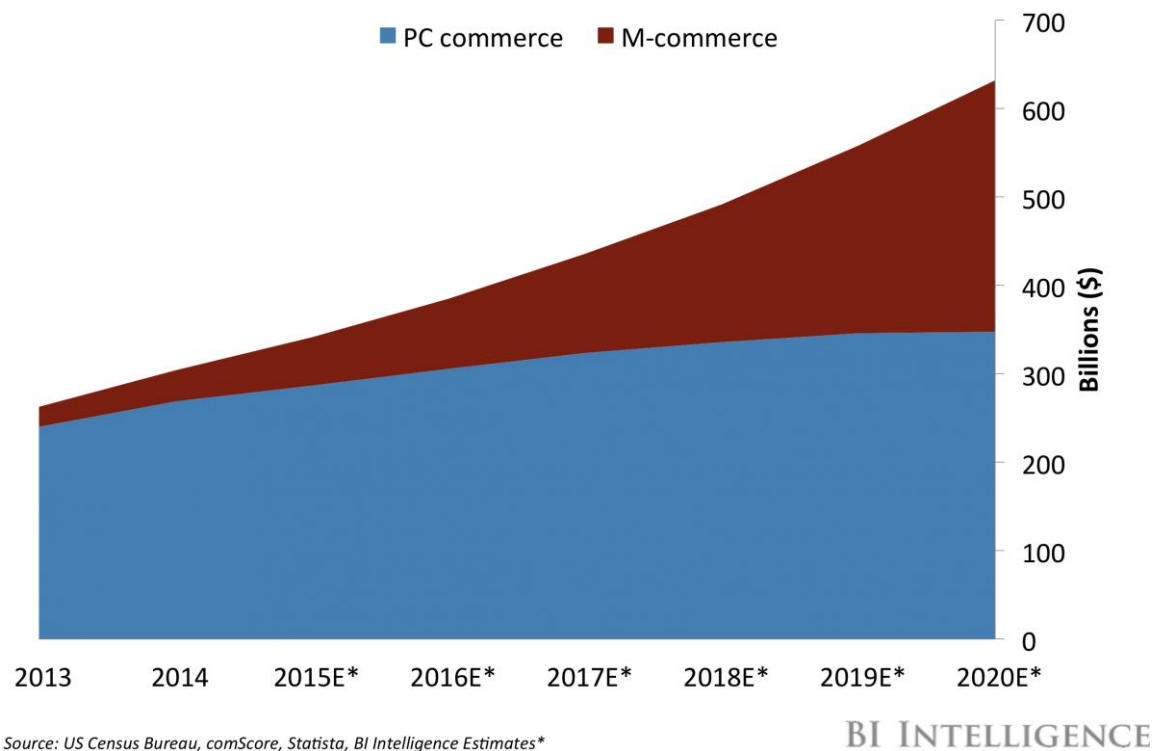
Source: Acuity Market Intelligence

BI INTELLIGENCE

BIOMETRICS SOLVE TWO PAIN POINTS FOR DIGITAL PAYMENTS

BI Intelligence forecasts that US e-commerce sales will hit \$631 billion in 2020, up from \$341 billion in 2015. And by 2020, nearly half of e-commerce sales are expected to come from phones. However, in order for digital payments to become mainstream, two major pain points in the mobile commerce experience will need to be addressed: a cumbersome user experience and rising potential for fraud.

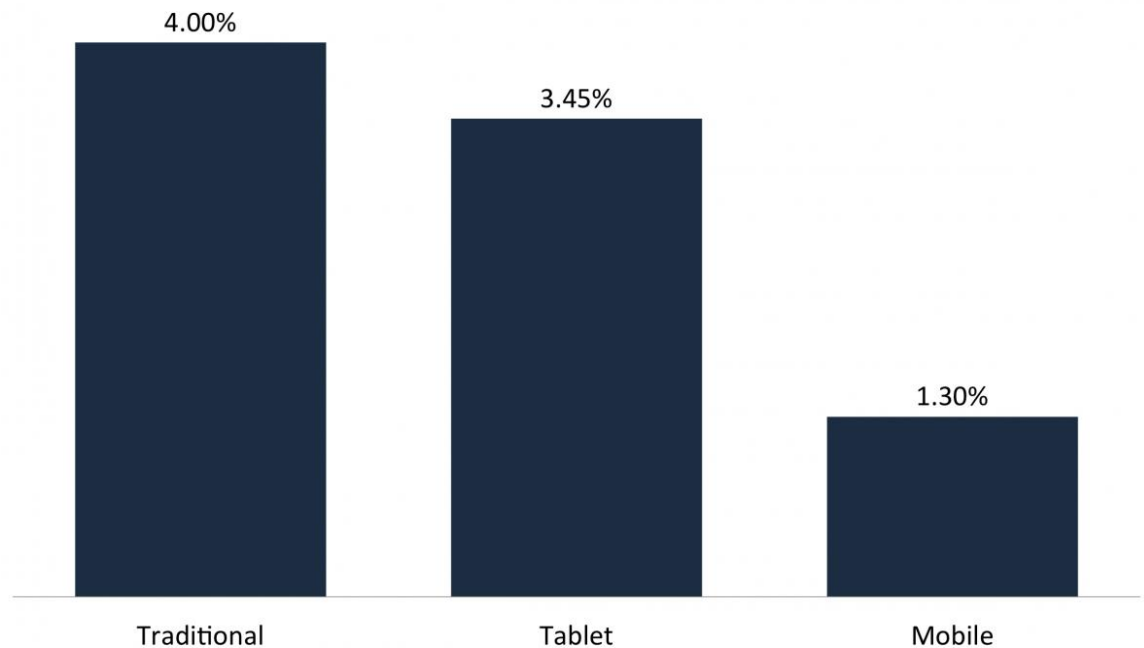
FORECAST: Mobile Share Of US E-Commerce Sales, 2013-2020



- **Making and authenticating purchases on mobile can be challenging.** Having to enter personal information and passwords through multiple steps on devices with small screens and slow connections can lead consumers to browse more than buy on these devices. Conversion rates on smartphones are 1.3%, compared with 4.0% on PCs, according to [Monetate](#). And additional security features, like 3D Secure, address verification, or security questions, while helping to protect consumers' financial data, also increase the number of steps between the user and checkout, further limiting purchasing.

US E-Commerce Conversion Rates, By Channel

Q4 2015

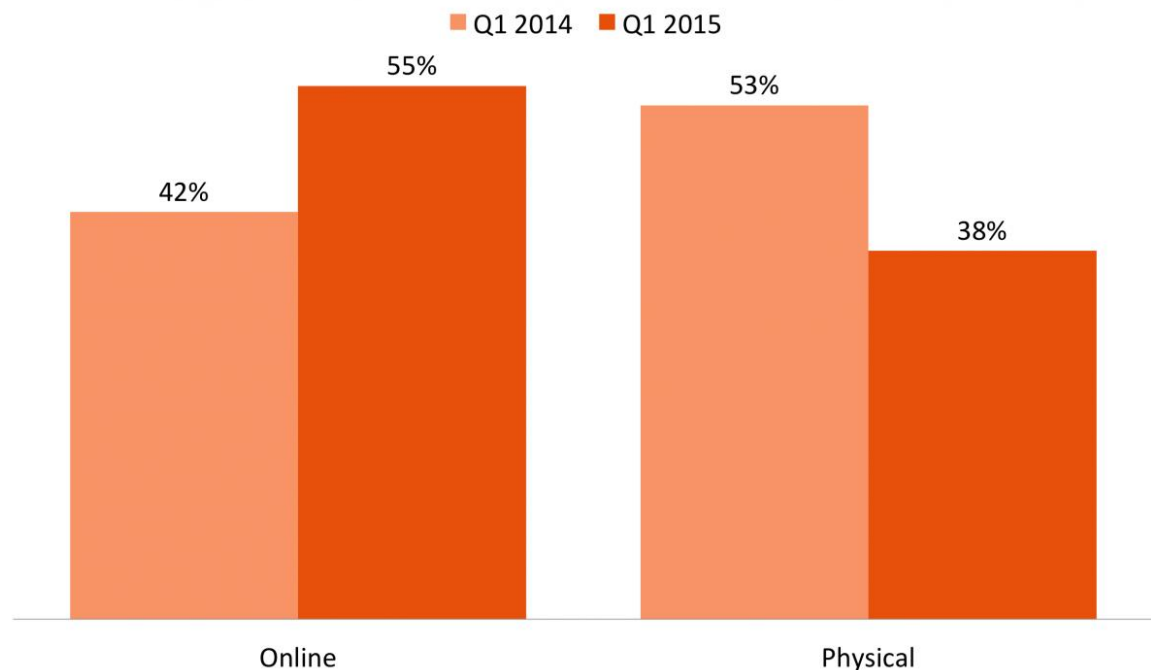


Source: Monetate

BI INTELLIGENCE

- **Fraud is becoming more prevalent online.** The widespread adoption of EMV-enabled chip cards has dramatically decreased counterfeit fraud at points of sale (POS) and cash machines — but that's pushing more fraud online. The majority of card-fraud costs among retailers now come from digital channels: 53% in Q1 2015, up from 42% a year prior, according to [LexisNexis](#). While merchants can easily check an in-store customer's photo ID if they suspect fraud, it's much more challenging to verify that an online customer is who they say they are — it's easy for thieves to access or guess verification information like addresses and passwords.

Percentage Of Card Fraud Costs For US Retailers, By Channel



**Figures do not add to 100% due to the omission of "other"*
Source: LexisNexis, n=58-176

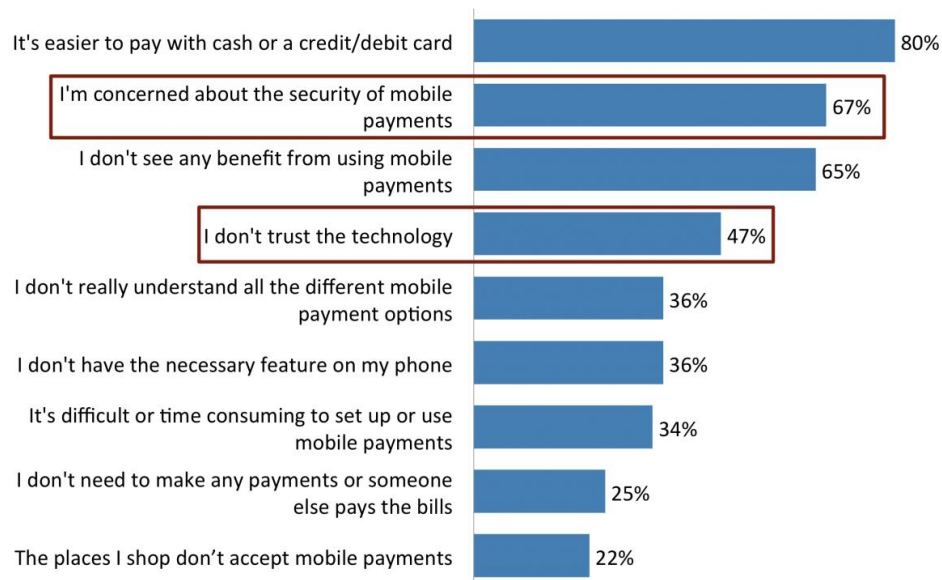
BI INTELLIGENCE

This is where biometric authentication comes in. It can make the mobile-purchasing experience easier and more secure.

- **A fingerprint or photograph can replace password entry and other steps, making mobile purchases simpler and faster.** Password entry alone is a significant pain point: 53% of shoppers forget their passwords more than once per week, which limits purchasing, according to [MasterCard](#).
- **Unique biological data is very difficult to fake, which provides greater protection for consumers and retailers.** Biometric authentication is less “hackable” than a password or secure PIN. It acts as an additional, more secure means of verification on top of CVV numbers, geolocation, and other authentication measures for online and in-person transactions. Added security could help mollify consumer fears about digital fraud, ease hesitation in adopting mobile payments, and mitigate fraud costs.
 - Two of the top five reasons that mobile phone owners cite for not using mobile payments are related to safety and security. As many as two-thirds of consumers polled in Q4 2015 by the [US Federal Reserve](#) said they're concerned about the security of mobile payments, and almost half don't trust the technology.

Top Reasons Consumers Don't Use Mobile Payments

Among US nonusers of mobile payments, Q4 2015



Source: US Federal Reserve, n=1,802

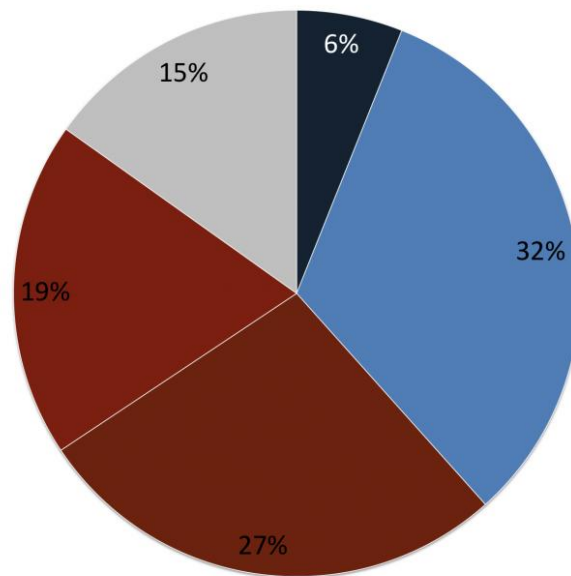
BI INTELLIGENCE

- The [US Federal Reserve](#) also found that 46% of consumers believe in-store mobile payments are somewhat or very unsafe, versus 38% who believe they are very or somewhat safe. Biometric authentication could therefore facilitate the adoption of mobile wallets like Apple Pay.

SURVEY: How safe do you believe personal information is when making in-store mobile payments?

US adults with mobile phones, Q4 2015

■ Very safe ■ Somewhat safe ■ Somewhat unsafe ■ Very unsafe ■ Don't know



Source: US Federal Reserve, n=2,244

BI INTELLIGENCE

METHODS OF BIOMETRIC AUTHENTICATION

Fingerprint identification is by far the most common biometric authentication method used today. It's integrated into iPhone and Samsung Galaxy devices, and a number of mobile apps rely on fingerprint ID to verify and secure various processes, including in-store and in-app purchases made via mobile wallets. iOS developers can build in Touch ID functionality to secure data.

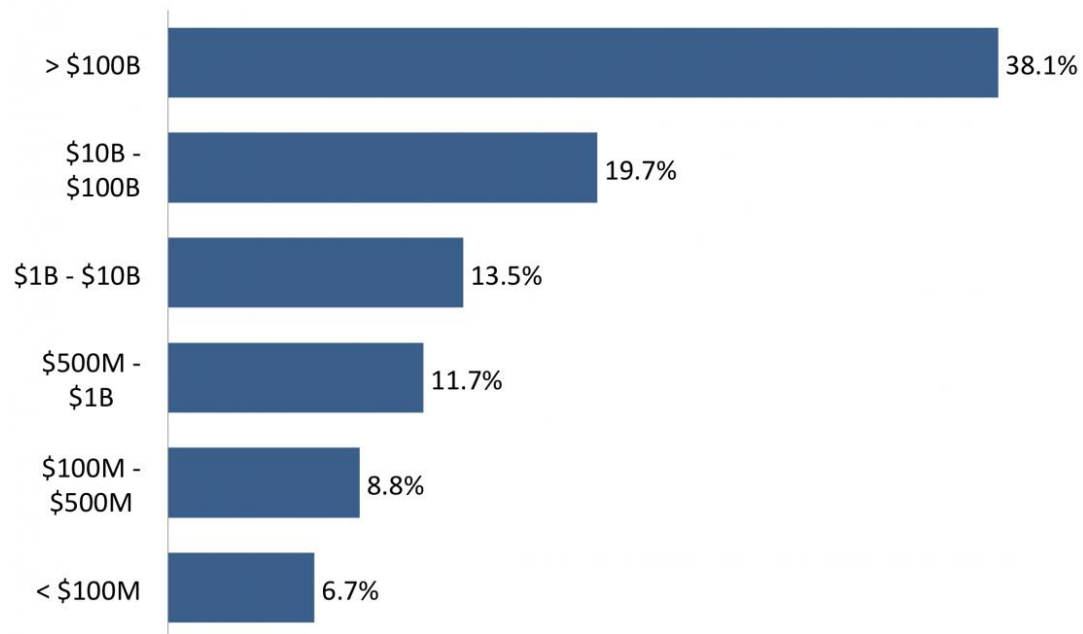
Here's how fingerprint ID works:

- **Fingerprint authentication scanners are built into phones or stand-alone devices.** The iPhone 5S and Samsung Galaxy S5, and subsequent versions of these devices, integrate sensors that capture high-resolution images of a fingerprint. Sensors are generally built into the phone's home button but can also be inserted under the liquid crystal display, or elsewhere. On iPhones, users place a thumb or finger on the home button to authenticate themselves, while Samsung users swipe a finger across a sensor located at the bottom of the phone. Stand-alone biometric authentication devices can also be installed at a physical point of sale. This allows biometric authentication to live on the merchant side, rather than only being possible through a consumer's personal device. While this type of biometric authentication is highly uncommon, it is something merchants could theoretically upgrade to. It raises additional privacy concerns, however, since biometric data might no longer be stored on an individual's device, but rather in a more centralized database.
- **Fingerprint data is encrypted and securely stored on the device.** The iPhone then stores the data in a "secure enclave," a processing environment separate from the rest of the phone. This makes it nearly impossible to retrieve the data even if a hacker gains access to the device. Android phones use a different but likely similarly secure method for fingerprint storage.
- **A software algorithm determines if a fingerprint is a match** after the user holds a finger on the scanner.

Fingerprints can already be used to unlock phones, verify mobile wallet payments, and open access to banking apps among other applications. Mobile wallets including Apple Pay, Android Pay, and Samsung Pay incorporate fingerprint authentication. And a growing number of financial institutions are offering customers the option to log into their apps with a fingerprint. Bank of America, Chase, and PNC all offer such functionality. And now it's becoming more widely available at smaller banking institutions as well. Research firm [Celent](#) found that as of January 2016, 608 financial institutions in the US offered fingerprint authentication in their mobile banking apps, up from just 252 in October 2015.

In addition, card networks including MasterCard are implementing the technology as part of the online payment process on mobile. And eventually, banks will likely grant access to secure terminals like ATMs via fingerprint scanners on customers' phones.






Percentage Of US Financial Institutions Offering App-Based Fingerprint Authentication, By Asset Amount *Q1 2016*



Source: Celent, n=608

BI INTELLIGENCE

Other biometric authentication methods include facial and voice recognition, vein prints, and iris scans. While far less common than fingerprint ID, some businesses are deploying these alternative methods for verifying identity.

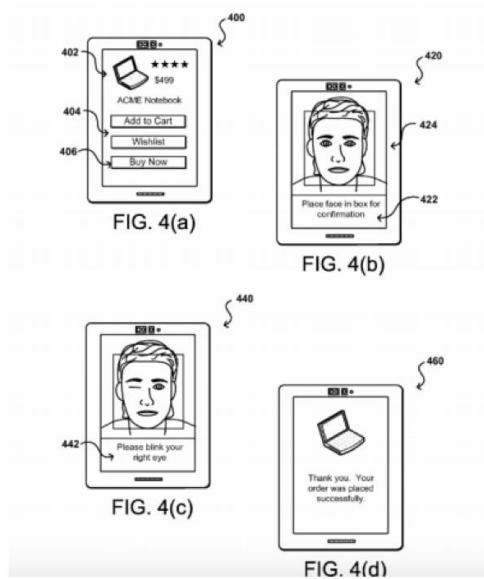
| NONFINGERPRINT BIOMETRIC IMPLEMENTATIONS | | | | |
|---|------------|----------------|---------------------|---|
| Brand | Product | Method | How It Works | |
|  | MasterCard | Identity Check | Facial recognition | Allows users to verify purchases with a selfie or eye-blink. |
|  | Amazon | Pay-by-Selfie* | Facial recognition | A patent that would allow users to verify account information with a selfie and action like blinking or smiling. |
|  | Citi | n/a | Voice recognition | Verifies users' identities by phone to ensure they are who they say. |
|  | WorldPay | FingoPay | Finger vein scanner | Allows users to register cards to their vein print and pay cardlessly by touching their finger to a vein scanner. |
|  | Diebold | Irving ATM | Iris scanner | Screenless ATM that verifies users' identities by scanning their iris. |

Source: Company data, US PTO, BI Intelligence

BI INTELLIGENCE

There are two basic types of alternatives to fingerprint biometric authentication that are gaining popularity.

- **Trait recognition:** Facial and voice recognition systems rely on a baseline photograph or voice print taken when a user signs up. For security, facial recognition systems generally require users to perform a function like blinking or smiling to foil impostors holding up a still photo. Businesses including MasterCard and Amazon (see figure) are testing or researching facial recognition, for use online or through cameras integrated into in-store POS terminals. Vocal recognition is intended to prevent fraudsters from accessing sensitive information over the phone. Citi, an early adopter, has said that it has registered 250,000 voiceprints thus far.



A diagram from Amazon's "pay-by-selfie" patent application

- **Alternate forms of body scanning.** Fingerprint identification has become fairly mainstream, and now firms are exploring other body scanning options like vein profiles and iris or retina scanners.
 - **Vein profiling.** Specialized scanners can read a user's unique "vein profile" using infrared technology to detect the pattern of veins. Finger vein technology (FVT) scanners are generally built into POS terminals rather than incorporated into a consumer-owned device. For example, [Sthaler's FingoPay](#) enables users to register a payment card to their finger vein template and then pay cardlessly by touching an FVT scanner at the point of sale. European processor WorldPay and Japanese bank Hitachi of Japan are testing the system.
 - **Retina and iris scanners.** ATM manufacturer Diebold recently launched Irving, a cardless, mobile-driven ATM that authenticates users through a retina scan rather than a PIN pad or password. Users enter all information via their phone, and then the ATM takes the retina scan and dispenses cash. Diebold has partnered with [EyeLock](#), a specialist in retina- and iris-based authentication hardware and software.

These biometric verification methods may well proliferate as consumers adopt new channels for transactions and new types of devices take off. Right now, most transactions take place via physical POS terminals, the consumer's desktop or mobile device, or ATMs. As connected devices like wearables, smart home products (e.g. smart refrigerators), and cars incorporate payment mechanisms, they will likely rely on various types of biometric verification.

BARRIERS AND RISKS

The biggest risks to using biometrics are associated with consumer privacy and data security. While the technology is seen as more secure than passwords and PINs, it also opens the door to some potentially serious problems that could hamper adoption.

- **Consumers can't change their biometric characteristics, unlike passwords or credit card numbers.** While biometric data is generally more heavily encrypted than passwords, if hackers do access a fingerprint or vein profile, for example, the victim can't avert future fraud by making a simple change, as they might by getting a new password or credit card. That is likely to concern or unnerve consumers — entrusting their biometric information to corporations like Apple or Google violates “commonly accepted notions of privacy and security,” according to [Scientific American](#).
- **Network effect.** Biometrics are unique identifiers, so using a single fingerprint is akin to using one password for every verification. If the data is breached, everything a consumer verified using that fingerprint is put at risk. Even worse, people have a finite number of biometric identifiers they can use, which limits their ability to update verification data after a breach.

There are also ways to evade or steal data from biometric sensors. Last August, [research from FireEye](#) uncovered a loophole in Android devices that enabled hackers to quietly collect data from fingerprint sensors, particularly with jail-broken phones. And various groups have found ways to bypass the fingerprint sensors in the iPhone [5S](#) and 6 by lifting a fingerprint and replicating it with latex.

Companies are using two primary mechanisms to help prevent large-scale breaches:

- **Decentralized storage:** Potential for a breach increases dramatically when data is stored in centralized locations, according to a [white paper](#) from PricewaterhouseCoopers. Businesses therefore tend to store data on consumers' devices rather on company servers.
- **Encryption and tokenization:** Biometric data is stored [separately](#) from other personal information on mobile devices. So even if the device is breached, hackers aren't likely to gain access to the data. And since the data is usually encrypted as well, a hacker who does manage to gain access would not easily be able to interpret it.

While security is the top priority if biometric authentication is going to become more common, there are other hurdles that biometric technology could face:

- **Regulation:** Countries have different regulations governing biometric data collection and storage, according to [PwC](#). Such rules could become more complex as new use cases for biometrics debut and could pose challenges as products are used across borders.
- **Fragmentation for users:** Users require consistency to form habits. If biometric devices are not broadly or uniformly implemented (e.g. using a fingerprint to make a payment in certain circumstances and a blink or vocal application in others), user adoption could be hampered, making integration less appealing for hardware and software vendors.
- **Fragmentation for developers:** Fingerprint scanners are accessed differently by different mobile operating systems, which could prove challenging for developers seeking to add the functionality to apps across iOS and Android devices. And outside of the phone space, it's difficult for developers to build integration for different kinds of hardware, like FingoPay or Irving, which could limit their uptake and adoption.

Biometric authentication that is easily accessible and integrated into user-based (rather than merchant-based) devices will be most likely to overcome these hurdles and take off.

Here's why:

- Biometric technology is already present in consumer devices, with fingerprint ID fairly widespread. Technology for merchant-based portals, like vein scanners at POS terminals or retina scanners at ATMs, is likely too expensive and too unfamiliar for vendors and consumers to comfortably adopt it in the near term.
- Consumers are more open to using biometric authentication on devices they already have. Nearly half of US and UK millennials surveyed by [Gigya](#) use one or more forms of biometric authentication, including fingerprint scanning, voice and facial recognition, or iris scanning. It's less challenging for consumers to adopt this familiar technology for new use cases than to adapt to something entirely new, like a vein scanner at the POS.

THE BOTTOM LINE

- US smartphone makers are rapidly integrating biometrics-based features, such as fingerprint scanners, into their devices.
- Global mobile biometrics market revenue, including sensor revenue from mobile devices, fees and revenues from biometric app downloads, and authentication-fee revenue from payment transactions, will reach \$34.6 billion in 2020, according to Acuity Market Intelligence.
- Biometric verification is a more secure solution for apps and devices compared with passwords and PINS and it also bypasses the need to remember a password.
- Fingerprints can already be used to unlock phones, verify mobile wallet payments, and open access to banking apps, among other applications.
- Biometric verification is largely concentrated on fingerprint-scanning technology on mobile phones, but the technology is expanding, and other verification methods, including facial recognition and iris scanning, are becoming more popular.
- While biometric technology is seen as more secure than passwords and PINs, it also opens the door to some potentially serious problems that could hamper adoption.

BI INTELLIGENCE

BI Intelligence, Business Insider's premium research service, provides in-depth insight, data, and analysis of everything digital. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key areas of tech: mobile, e-commerce, digital media, payments, the Internet of Things, and more.

If your organization would like to learn more about our research, including a license to republish our charts, please contact: intelligence@businessinsider.com

**Copyright © 2016 Business Insider, Inc. All Rights Reserved.
Proprietary and Confidential Property of Business Insider, Inc.**

If you are an authorized user in an organization with a corporate license, your use of the report is subject to the terms and conditions executed between your organization and Business Insider, Inc. Otherwise, your use of the report is subject to the terms and conditions located at <http://www.businessinsider.com/terms> ("Terms Of Use") and the following additional terms:

You are granted a nonexclusive, nontransferable, limited right to access and use the report for research purposes. This right is granted to you for your individual use only. You acknowledge that this report and the contents thereof are the intellectual property of Business Insider, Inc. or its licensors. You further acknowledge that nothing in these terms shall constitute a sale or transfer of title or ownership from Business Insider, Inc. to you of any rights in and to the report. You shall not infringe, or enable the infringement of, the intellectual property rights of Business Insider, Inc. in any way, including, without limitation, by making available to other individuals externally or internally, forwarding via email, posting on a publicly accessible website, posting on internet or intranet, directly or indirectly reproducing, downloading, or otherwise distributing (in any form, current or yet to be developed) the report or any portion thereof without prior written permission of Business Insider, Inc.

Notwithstanding the foregoing, you may use data and information provided in the report in (a) external presentations to customers and licensees and potential customers and licensees; (b) presentations at conferences and events where you are a featured speaker; (c) earnings calls, analyst days and other investor presentations. All rights not explicitly granted to you herein are reserved to Business Insider, Inc. If there is a conflict between these additional terms and the Terms Of Use, these additional terms will control for that conflict.