Biometric Authentication in Payments

CONSIDERATIONS FOR POLICYMAKERS

November 2017
# Contents

1  Executive Summary ........................................... 5

2  Overview of Biometric Authentication ................. 7
   2.1  What Are Biometrics? ................................. 7
   2.2  What Is Authentication? .......................... 7
   2.3  How Does Biometric Authentication Work? .... 8
   2.4  Biometric Authentication Modalities .......... 9

3  Drivers of Biometric Adoption ......................... 11
   3.1  Advancements in Technology .................... 11
   3.2  Increasing Consumer Familiarity and Demand 12
   3.3  The Dramatic Rise of Mobile Devices .......... 13
   3.4  Dual Objectives: Security and Convenience 14
   3.5  Government Focus on Identity Verification & Financial Inclusion 15

4  Biometrics in the Payments Ecosystem .............. 16
   4.1  Outlook for the Use of Biometric Authentication 16
   4.2  Benefits of Biometric Authentication for Payment-System Participants 17

5  Selected Deployments of Biometric Authentication in Payments and Financial Services .... 18
   5.1  The Americas ...................................... 19
   5.2  Europe ............................................ 20
   5.3  Africa and the Middle East ..................... 21
   5.4  Asia-Pacific ....................................... 22

6  Biometrics Legal Landscape .......................... 23
   6.1  Overview of Biometrics-Related Laws ........... 23
   6.2  Applying Laws to Rapidly Evolving Technologies Such as Biometrics 26
7 Advancing Biometric Authentication: Issues for Further Attention 26

7.1 Standardization and Interoperability 26
7.2 Layered, Risk-Based Approaches to Payment Security 27
7.3 Data Security – Storage and Transmission 27
7.4 Consumer Privacy 29
7.5 Accessibility and Inclusion 29

8 Guiding Principles on Biometric Authentication for Policymakers 30

8.1 Foster Stakeholder Dialogue and Engagement 30
8.2 Support Industry-Driven Standards and Interoperability 31
8.3 Reframe Security Discussions to Reflect New Technology Developments 31
8.4 Provide Legal Clarity for Payment-System Participants 32
8.5 Lead by Example 32

9 Conclusion 33

Appendix
Selected Organizations Working on Biometric Issues in Payments 34

Endnotes 37
About Promontory Financial Group

Promontory Financial Group, an IBM Company, excels at helping clients resolve critical issues, particularly those with a regulatory dimension. Promontory professionals have unparalleled regulatory experience and insight, and provide our clients with frank, proactive advice informed by best practices and regulatory expectations. Founded in 2001 by Chief Executive Officer Eugene A. Ludwig, former U.S. comptroller of the currency, Promontory became a wholly owned subsidiary of IBM in 2016. More at promontory.com

About Visa

Visa Inc. (NYSE: V) is the world’s leader in digital payments. Our mission is to connect the world through the most innovative, reliable and secure payment network – enabling individuals, businesses and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second. The company’s relentless focus on innovation is a catalyst for the rapid growth of connected commerce on any device, and a driving force behind the dream of digital payments for everyone, everywhere. As the world moves from analog to digital, Visa is applying our brand, products, people, network and scale to reshape the future of commerce. For more information, visit usa.visa.com/aboutvisa, visacorporate.tumblr.com and @VisaNews.

Visa’s Global Public Policy group, established in 2015, commissioned this study. The group’s mission is to inform public policy dialogue globally through thought leadership.
Biometrics have gained popularity as an authentication tool in a number of industries and contexts, including the financial services sector. Technology developments – notably, improved accuracy and lower costs of biometric solutions, coupled with the dramatic rise of mobile devices globally – have served as key drivers.

Business and consumer demand for secure, convenient payment options in today’s changing fraud landscape has also played an important role.

More broadly, biometrics represent one part of a growing tapestry of data on individuals and their transactions – including personal data, geolocation information, and device IDs – available to support new and enhanced authentication services.

As the use of biometric authentication has grown, governments and consumer groups have raised important public policy questions about data security and privacy issues. Businesses have also posed questions about standardization and interoperability in the biometric authentication landscape. These issues, and many others, have distinct implications when considering the growing application of biometric authentication in payments. What role can biometrics play in promoting both innovation and security? Are these two goals in conflict with each other? Addressing these questions will be key to the further advancement of biometric authentication in payments.

This paper leverages Promontory’s experience with financial services and risk management to outline the benefits of biometric authentication and issues for further attention by payment-system stakeholders. It also suggests activities that government agencies, lawmakers, regulators, and other rulemaking bodies (collectively, policymakers) may take to support the continued development of biometrics as an authentication tool in the payments industry.

Policymakers hold a powerful and unique position with great ability to influence the further development of biometric authentication. This paper proposes five specific guiding principles for policymakers to consider as they deepen their understanding of biometric authentication’s evolving role in the payments ecosystem.
## Guiding principles on biometric authentication for policymakers

<table>
<thead>
<tr>
<th>GUIDING PRINCIPLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>FOSTER STAKEHOLDER DIALOGUE AND ENGAGEMENT</strong></td>
<td>Multi-stakeholder dialogue on evolving technologies such as biometric authentication solutions helps bring a range of voices to discussions that support advancements in the payments ecosystem. By engaging with a variety of payment-system participants, policymakers can deepen their understanding of technology trends, stakeholder perspectives, and potential congruence with policy objectives.</td>
</tr>
<tr>
<td>2. <strong>SUPPORT INDUSTRY-DRIVEN STANDARDS AND INTEROPERABILITY</strong></td>
<td>Standards support payments innovation by making it easier for all parties in the payments ecosystem to adopt and deploy new technologies. Interoperability provides the foundation for open and accessible payment systems, creating efficiencies that benefit all ecosystem stakeholders. By supporting interoperability and industry-led, principles-based standards not tied to a specific technology, policymakers ensure a lasting framework that can keep pace with both innovation and changing risks in the payments landscape.</td>
</tr>
<tr>
<td>3. <strong>REFRAME SECURITY DISCUSSIONS TO REFLECT NEW TECHNOLOGY DEVELOPMENTS</strong></td>
<td>Historically, many have viewed security and convenience as competing priorities. Biometric authentication, however, presents an opportunity to develop solutions that provide more convenience to consumers while also enhancing security. The next generation of authentication toolkits are being designed to support a layered, risk-based approach to payment security with complex verification methods that are difficult for criminals to steal and deploy. Policymaker guidance that reflects technology developments and evolving security strategies can strengthen payment-system security, allowing ecosystem participants to leverage innovative solutions and approaches to mitigate risk.</td>
</tr>
<tr>
<td>4. <strong>PROVIDE LEGAL CLARITY FOR PAYMENT-SYSTEM PARTICIPANTS</strong></td>
<td>By engaging in multi-stakeholder discussions on legal issues related to biometric authentication – such as data storage, usage, and transmission – before the passage of legal measures, policymakers can help build consensus around governance objectives, including assessing whether non-legislative responses such as industry standards may be sufficient. Where existing laws differ or conflict between jurisdictions, policymaker coordination can support a more efficient and certain operating environment for entities in the payments system.</td>
</tr>
<tr>
<td>5. <strong>LEAD BY EXAMPLE</strong></td>
<td>Policymakers and governments can send a positive message to consumers and businesses alike by embracing biometric technology in their own products and services, as appropriate in their market.</td>
</tr>
</tbody>
</table>

The next section provides an overview of biometric authentication, including key definitions and examples of biometric modalities. Section 3 summarizes drivers of biometric adoption globally, including discussion of technology developments, consumer preferences, and congruence with government policy objectives. Section 4 highlights the outlook for biometric authentication and describes how biometrics are impacting payments. Section 5 provides examples of biometric deployments in payments and financial ser-
vices around the world. Section 6 offers an overview of the legal landscape surrounding biometrics, including the application of existing data-security and/or privacy laws to the context of biometrics. Section 7 describes issues for further attention in the biometric authentication landscape, including standardization and interoperability, layered risk-mitigation strategies, data security, consumer privacy, and accessibility and inclusion. Finally, Section 8 provides more detail on these guiding principles on biometric authentication, outlining how policymakers can play a critical role in advancing biometric authentication in their markets.

2 Overview of Biometric Authentication

This section provides an overview of biometric authentication, including key definitions and examples of biometric modalities.

2.1 What Are Biometrics?
Biometric identifiers (biometrics) are unique, intrinsic physical or behavioral characteristics that can be used to identify or verify the identity of an individual. They are categorized as either physical or behavioral.

<table>
<thead>
<tr>
<th>Physical</th>
<th>Behavioral</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual biological or physiological traits such as fingerprints, facial characteristics, and iris patterns.</td>
<td>Traits that describe how individuals operate or function, such as signatures, keystroke patterns, or gait.</td>
</tr>
</tbody>
</table>

Law enforcement and government agencies have long used fingerprints to identify individuals in criminal cases. Even today the most common trait used for biometric recognition is the fingerprint. However, iris and facial recognition technologies are increasingly common. As the accuracy of these technologies increases and the costs decrease, their use continues to grow.

2.2 What Is Authentication?
Authentication is the process of verifying that individuals or entities are who they claim to be. There are three main mechanisms for authentication:
2.3 How Does Biometric Authentication Work?

Biometric authentication includes two key phases: enrollment and verification, as illustrated in the following graphic.

During enrollment, the individual’s biometric data is captured, converted into a “template,” and stored, either locally on a device or centrally on a server. An individual’s identity should be verified, such as by government identification or other reasonable means, prior to biometric data collection to ensure the integrity of the enrollment process. The stored biometric template is a coded digital representation of patterns extracted during the template generation process. During verification, the individual provides his or her biometric data via a sensor or reader, and the collected biometric template is compared to the stored template. If a match occurs, the individual is successfully authenticated.

As biometric systems have matured, accuracy has improved. Declining error rates have enabled biometrics to become an effective authentication mechanism in many payment use cases. As with other authentication
methods, error rates vary based upon a number of factors, notably the modality used and the maturity of the technology. Errors typically fall into one of two categories – false accepts or false rejects. A “false accept,” or false positive, occurs when the system determines that an authentication template from one individual matches an enrollment template from another individual. A “false reject,” or false negative, occurs when the system determines that an authentication template and an enrollment template from the same individual do not match. The rate of false accepts is referred to as the “false accept rate” (FAR) and the rate of false rejects is referred to as the “false reject rate” (FRR).

2.4 Biometric Authentication Modalities

Modality refers to the trait used for authentication. Selecting an appropriate modality to use in a biometric authentication system depends on a host of factors, including the type of technology used for its deployment and the application in which it will be used. Performance, usability, and cost effectiveness of the biometric solution depend on technology maturity and other factors, which vary across modalities. The following table highlights common types of authentication modalities and provides examples of applications in the payments ecosystem.

<table>
<thead>
<tr>
<th>MODALITY</th>
<th>DESCRIPTION</th>
<th>EXAMPLES/DEVELOPMENTS IN THE PAYMENTS ECOSYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>Identifies individuals using the ridge-valley patterns present on fingers.</td>
<td>Recent deployments include mobile wallets such as Apple Pay, Android Pay, and Samsung Pay; ATMs enabled with Apple’s Touch ID; and pilots of contactless payment cards integrated with fingerprint sensors.</td>
</tr>
<tr>
<td>Face</td>
<td>Identifies individuals using their facial characteristics such as shape of facial features and skin texture.</td>
<td>Visa has partnered with Banco Neon in Brazil to offer online authentication using facial recognition. Mastercard’s “Pay by Selfie” and Alibaba’s “Smile to Pay” allow users to authenticate payment transactions by taking a selfie.</td>
</tr>
<tr>
<td>Iris</td>
<td>Identifies individuals using the detail-rich, intricate pattern of the iris.</td>
<td>Two major South Korean banks, KEB Hana Bank and Woori Bank, announced plans to employ an iris recognition solution to authenticate bank customers in the mobile environment.</td>
</tr>
<tr>
<td>Palm and Finger Vein</td>
<td>Identifies individuals using the vein pattern inside their palms or fingers.</td>
<td>Brazilian and Japanese banks have used palm and finger vein authentication technologies for ATMs. Tokyo’s plans for the 2020 Olympics include a system where tourists will pay for goods and services using only biometrics, including vein scanning and fingerprint biometrics.</td>
</tr>
</tbody>
</table>
## Voice Recognition

Identifies individuals based on voice characteristics such as the pitch, tone, and rhythm of their speech.  

In the U.S., USAA Bank’s mobile application allows users to use voice, fingerprint, or facial recognition as a biometric layer of authentication.  

Wells Fargo’s Commercial Electronic Office (CEO) mobile application offers voice biometric authentication, allowing users to authenticate themselves using their mobile phone’s front-facing camera and microphone in lieu of passwords.  

Biometrics companies Agnitio and VoiceVault have integrated their technologies for card-not-present payment transactions. They both supply biometric technology that analyzes the audio to authenticate the user’s identity.

---

### BEHAVIORAL BIOMETRICS

<table>
<thead>
<tr>
<th>MODALITY</th>
<th>DESCRIPTION</th>
<th>EXAMPLES/DEVELOPMENTS IN THE PAYMENTS ECOSYSTEM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keystroke</td>
<td>Identifies individuals based on the manner and rhythm in which they type character sequences on a keyboard (virtual or physical).</td>
<td>The use of keystroke biometrics for authentication remains somewhat limited, as companies have expressed concern about its efficacy as a stand-alone solution. However, researchers believe that it may serve as a complement to traditional username/password combinations, where the user is granted access if he/she is also able to type a few words of a pass phrase within a reasonable threshold of latency variability (keystroke duration, finger placement, and applied pressure) from the reference signature.</td>
</tr>
<tr>
<td>Gait</td>
<td>Identifies individuals based on the manner in which they move in space (typically while walking).</td>
<td>Google’s Project Abacus represents an effort to move away from traditional passwords and PINs in favor of a combination of mobile-device measurements to authenticate the identity of a user. The project is intended to identify an individual by considering several biometric measurements, including gait.</td>
</tr>
<tr>
<td>Heartbeat</td>
<td>Identifies individuals based on their electrocardiogram (ECG), a measurement of the electrical activity of the heart.</td>
<td>Royal Bank, TD Bank, and Mastercard tested electrocardiogram identification using a wristband designed by a Canadian authentication solutions company, Nymi, to make secure online payments. With the increased use of wearables, heartbeat analysis may have interesting future use cases. For example, researchers believe that heartbeat biometrics could be used by individuals to protect electronic health records and conveniently and quickly provide medical staff access to such information.</td>
</tr>
</tbody>
</table>

---

1 Voice or speech recognition can be viewed as both physical and behavioral biometrics, as the authentication method involves characteristics of both.
Each of these modalities may be deployed as part of a layered, risk-based approach to payment security. Emerging authentication solutions are exploring the possibility of combining multiple biometric authentication technologies and/or layering with non-biometric solutions. For example, Visa partnered with Safran Identity & Security and Delta ID to build a prototype that incorporates iris scanning and facial recognition technology into Visa Checkout, the network’s online payments service. Other emerging solutions incorporate physical location of the cardholder, and behavioral and contextual data, like IP address and device ID, into the authentication process. One biometric modality can also serve as a backup for another biometric modality (e.g., a user who does not have a smartphone with fingerprint recognition could use another authentication measure such as face or voice recognition as a default and/or backup option).

3 Drivers of Biometric Adoption

Several factors have driven the increased use of biometric authentication over the past few years. Technological developments, notably improved accuracy and lower costs, have played a key role. Demand from consumers and businesses for convenient and secure authentication solutions has also served as a driving force, bolstered by growing mobile-phone adoption in many markets. In addition, governments have pursued the use of biometrics to deliver on policy objectives such as expanding financial inclusion and reducing identity theft. Several of these factors are described below.

3.1 Advancements in Technology

As biometric technologies have matured and improved – becoming more accurate and cheaper – they have become a cost-effective option for a growing number of use cases. And as with other digital technologies, the rapid rise of mobile-device availability and use has accelerated the advancement of biometrics.

Rapid Improvement in Sensor Quality and Accuracy

As recently as the early 2000s, biometric technology lacked the consistent accuracy and ease of use necessary for widespread commercial applications. For example, tests of several biometric devices conducted and reported in 2000 showed actual FARs ranging from 0% to 6% and FRRs ranging from 8% to 70%, indicating relatively high and varied rates of false accepts and rejects. Sensors were once difficult to control, thwarted by minor variances that would obscure captured data. Early biometric deployments frequently had trouble extracting the minutiae of a fingerprint, which would undermine the entire authentication process. Early technology also operated at much slower speeds.
The accuracy and performance of biometric sensor technology have increased considerably in recent years. Today, many consumer mobile devices are capable of scanning fingerprints with ease and are equipped with cameras and microphones so powerful that they can capture data at minute levels. Wells Fargo Bank’s eye-scan technology, for example, works so quickly that the developers had to slow it down so that customers would know it had actually registered their identities. Citibank’s voice-recognition system takes only 15 seconds to capture enough information about a customer’s vocal patterns to validate his or her identity. This voice imprint template shortens the time that customers spend identifying themselves to a Citibank call-center representative, with traditional methods typically taking 45 seconds. Despite these improvements, accuracy of biometric systems depends on a number of factors, such as the type of biometric data used, the maturity of the technology, and environmental conditions (e.g., noise for the voice modality and lighting conditions for the face modality).

**Decreasing Costs**

Lower implementation costs have also driven the increased use of biometrics. Before biometric sensors became widely available through smartphones, implementation costs were prohibitively high, with sensors costing thousands of dollars to install; the required large-scale data storage added further expense. To capture biometrics, companies had to pay to distribute the necessary technology to tens of millions of customers, and the lack of industry standardization contributed to the high cost. In comparison with other authentication measures such as passwords and PINs, the costs outweighed the benefits in most cases.

Today, less expensive sensors in smaller forms allow modalities that were previously too expensive to develop and too large for mass deployment to be available to millions of users via mobile devices. More complicated modalities, such as behavioral biometrics, are also poised to grow. Although only 22% of U.S. companies currently use behavioral biometrics, 54% plan to implement behavioral biometrics in the future, with decreasing costs making these technology applications more economically feasible.

**3.2 Increasing Consumer Familiarity and Demand**

The ease and convenience of biometric authentication, in addition to its security advantages, are powering its rapid growth and adoption. For example, many consumers adapt with relative ease to authentication methods that seem familiar, such as selfie-like facial recognition and fingerprint recognition that require only a touch of a button on a smartphone. Fingerprint recognition is now the form of biometric payment most favored by European consumers for its ease of use and security. When asked how secure they think an authentication method is, over 81% of European consumers said they view fingerprint authentication as a secure form of payment, followed by iris scanning at 76%. Authentication occurs within seconds, and some modalities like iris recognition can be used without physical contact.

Previously, the inconsistent accuracy, high manufacturing cost, and
fragmented deployment of biometric authentication yielded a limited number of commercial applications. As a result, consumers only rarely encountered biometrics, and thus were relatively unfamiliar with the technology. Naturally, consumers were averse to entrusting unfamiliar technology with their personal data, even after the technology became more accurate and secure. Over the years, several large-scale biometric deployments helped carry the technology into the mainstream in a number of markets – for example, implementation of vein readers at ATMs in Japan and Brazil in the mid-2000s and the inclusion of Touch ID in the Apple iPhone 5S, launched in 2013 in multiple countries. In September 2017, Apple introduced its own facial-recognition program, Face ID, that unlocks its new iPhone X, replacing the Touch ID fingerprint authentication system on many of its other models. Given Apple’s influence in the mobile industry, its move to promote facial recognition could raise the profile of this biometric authentication modality.

### 3.3 The Dramatic Rise of Mobile Devices

Rising mobile-phone use and improved mobile technology have also played key roles in driving the adoption of biometrics. Increasing levels of commerce and communications are taking place over digital and mobile channels. For example, in 2017, 77% of Americans owned a smartphone, compared to 35% in 2011. Many smartphones now have high-quality biometric sensors, making the technologies for biometric collection more widely available and literally placing them in the hands of users.

In 2013, the biometric landscape changed completely with Apple’s launch of the iPhone 5S, which came equipped with Touch ID, a fingerprint sensor and biometric-matching software. Consumer trust in the Apple brand, coupled with the device’s ease of use, triggered a wave of consumer and business interest in the technology. Soon after the release of the iPhone 5S, other manufacturers rushed to build and promote their own devices equipped with fingerprint authentication, such as Samsung with its Galaxy S5...
phone. According to Apple, 89% of users with Touch ID-enabled iPhones use the fingerprint scanner to unlock their devices. This feature can also be used by individuals to access accounts and confirm payments or transactions via their mobile devices. Acuity Market Intelligence estimates that nearly 1 billion biometric smartphones were in use in 2016, representing 40% of the global smartphone market. Acuity expects this percentage to grow to 100% of the 2 billion smartphones shipped annually within two years, reaching 100% installed-base penetration by 2022. Fingerprint scanning leads authentication methods in customer confidence, in both the proportion of consumers who believe it to be effective (49%) and consumers willing to use the solution (65%). Fingerprint scanning also appeals to customers because of its nearly frictionless experience, especially as deployed in Touch ID, where the iPhone typically unlocks within a second of placing a finger on the phone’s home button.

New modalities are being tested as well. The Samsung Galaxy S8 smartphone features facial-recognition and iris-scanning biometric authentication methods. Mobile growth also extends to wearables such as smartwatches and fitness activity trackers, which are equipped with sensors that enable the electronic collection and exchange of biometric data with other devices. Gartner, Inc., a technology research and advisory firm, predicts that 50% of consumers in mature markets will use smartphones or wearables for mobile payments by 2018. Wearables offer unique benefits as authentication devices, as they have the ability to collect behavioral biometric data on a near-continuous basis.

3.4 Dual Objectives: Security and Convenience

Proliferation of data and emerging technologies are enabling new secure and convenient authentication methods. Biometrics complement traditional forms of authentication such as passwords and PINs – which, while familiar, are susceptible to being forgotten, lost, hacked, or skimmed. Researchers recently found that requirements for frequent password changes meant to increase access security actually result in weaker security. Complicated passwords are easily forgotten, as well as inconvenient to reset. As an authentication method, biometrics are more complex, making them more difficult to operationalize for fraud. And, because biometrics are inherent to the account holder, they can’t be forgotten.

As fraudsters have grown more adept at targeting traditional authentication data points, the payments industry has developed new technologies to enhance security in the ecosystem. For example, the adoption of EMV-enabled chip cards has helped decrease fraud at the card-present point of sale (POS). However, fraud in the card-not-present (CNP) environment is increasing due, in part, to authentication challenges for online transactions. For CNP transactions, biometrics could improve customer authentication compared with more common methods such as static passwords and security codes (i.e., the three- or four-digit code on the front or back of most credit and debit cards). For example, consumers could authenticate online transactions using their face through their device camera, via voice through the device microphone, or using the device’s integrated fingerprint reader. Biometrics can also be deployed to improve authentication for mobile-based
Biometric Authentication in Payments

3.5 Government Focus on Identity Verification & Financial Inclusion

As biometric technologies have become more affordable and widespread, governments have turned to them to pursue social policies such as delivering public services more efficiently, combatting fraud within benefits programs, and bringing more people into the formal economy. A number of governments are implementing or exploring digital identity programs that incorporate biometrics. With over 1 billion participants enrolled, India’s Unique Identification Authority of India (UIDAI), also known as the Aadhaar project, maintains the world’s largest biometric database. Citizens receive a unique identification number linked to their fingerprints and iris scans, which are collected during an enrollment process and stored in a central repository. The scheme helps identify those entitled to government services, as well as those fraudulently receiving benefit payouts. Other countries such as Nigeria and Tanzania are studying the Aadhaar scheme to assess the potential benefits of migrating to biometrics to expand identity verification and social services to their citizens.

Governments around the world are increasingly turning to biometric-identity management systems to protect citizens from identity theft and help prevent criminals and terrorists from using fraudulent identification documents. In a number of U.S. states – including Illinois, New York, and California – governments are fighting fraud by incorporating facial-recognition technology into the identification processes used by their Departments of Motor Vehicles. In Illinois, the technology supported a database of facial-recognition information that helped detect thousands of fraud cases, including financial crimes and, on occasion, auto-theft rings, gang activity and welfare fraud. In many cases, fraudsters were using multiple identities to commit crimes and escape detection.

Financial institutions and governments are also leveraging biometrics to advance the financial inclusion of underserved and unbanked populations. According to the World Bank, around 2 billion people across the globe do not use formal financial services and more than 50% of adults in the poorest households are unbanked. Biometrics can help overcome fundamental challenges to financial inclusion (e.g., unbanked people may not have the formal identity cards required by financial institutions). Coupled with tiered payments. In the U.S., the Federal Financial Institutions Examination Council (FFIEC) notes that financial institutions may consider leveraging biometrics to enhance authentication for mobile financial services.

These technologies are being pursued to augment the evolving toolkit of authentication options available to financial institutions, merchants, and other businesses. Technology advancements can provide a broader range of data elements for authentication purposes – not only biometrics, but other data points such as IP addresses and device IDs. This additional information provides opportunities to enhance layered approaches to payment security with complex verification methods, which can strengthen defenses against data breaches and fraud.
know-your-customer requirements, biometrics can facilitate a smoother identity verification process for unbanked consumers. There are challenges to consider, however, including the cost of the biometric-related product (which may impact affordability for unbanked communities) and connectivity issues (which may impact reliability).

4 Biometrics in the Payments Ecosystem

This section describes the outlook for the use of biometric authentication and presents selected examples of biometric deployments in payments around the world.

4.1 Outlook for the Use of Biometric Authentication

The outlook for the use of biometric authentication in payments is positive. Biometrics are, in many ways, an ideal authentication solution for consumer payments – offering both convenience and security. The popularity of biometric technology as both a security measure and a tool of convenience is expected to drive its commercial growth, especially in trusted industries such as the financial sector.

Value of Biometrically Verified Smartphone Payment Transactions, Per Annum in Millions, 2016-2021

Goode Intelligence predicts there will be 1 billion users of mobile biometrics for financial services by 2020 – a 300% increase from 2015.\(^\text{17}\)
4.2 Benefits of Biometric Authentication for Payment-System Participants

Biometric technologies offer tangible benefits for payment-system participants, such as a more convenient payment experience and enhanced security, particularly when used as part of a layered approach to payment security that is commensurate with the risk presented. The following chart summarizes the key existing and potential future benefits of biometric authentication for payment-system participants:

| Consumers | Security: Compared to passwords and PINs, authentication methods such as biometrics enhance security for consumers by making it more difficult for criminals to steal and deploy payment data. |
| Merchant | Convenience: Over 40% of Europeans say that biometric authentication could eliminate the need for multiple passwords and PINs. Because biometrics are inherent to the account holder, they can’t be forgotten. Biometrics can also streamline cardholder verification for operational processes (e.g., leveraging voice recognition to authenticate customers contacting a call center), limiting the use of weaker identity-verification solutions such as security questions and reducing customer frustration with the authentication process. |
| Financial Institutions and Payment Providers | Security: By strengthening their payments environment through complex authentication solutions like biometrics, merchants can strengthen their defenses against data breaches and fraud. |
| Polymakers and Governments | Improved Customer Experience: Biometrics can reduce friction in payment transactions and improve the customer experience in both in-store and online transactions, helping to generate more sales. Subject to applicable privacy laws, using biometrics can also help merchants differentiate their services to consumers looking for more convenient and secure payment options. |
| | Security: Financial institutions and other payment providers can leverage biometrics to enhance security for payment transactions and operational processes involving customer authentication, as well as to limit false declines. |
| | Improved Customer Experience: The improved customer experience tied to biometrics can lead to higher card usage, helping generate more revenue for financial institutions and other payment providers. Using biometrics can also help these entities differentiate their services to consumers and businesses looking for more convenient and secure payment options. |
| | Security: The use of biometrics in the payments ecosystem can help governments meet policy objectives, including enhancing security and trust in the payments ecosystem. By making it more difficult for fraudsters to steal and deploy payment information, biometrics can support policymaker goals of preventing breaches of payment-card data and combatting fraud. For example, biometrics can help with proof of life for welfare, pension and other government disbursements. |
| | Promoting Electronic Payments: By making payments more convenient and seamless, biometrics can help drive the adoption of electronic payments and enable digital and mobile commerce. |

Juniper Research expects that biometrics will be used for over 18 billion transactions by 2021, growing at a compound annual growth rate of 83.7% from 2016 levels. Juniper also expects that the value of biometrically verified smartphone payment transactions across the globe will exceed $210 billion in 2021.
Realizing these benefits requires cooperation across stakeholders. Cooperation can help foster trust across ecosystem participants and incentivize the significant investments required to support the ongoing development of biometric authentication technologies.

5 Selected Deployments of Biometric Authentication in Payments and Financial Services

Biometric authentication technology is deployed for various uses in the payments ecosystem across the world. Several regions in particular have undertaken extensive biometric implementations. These have included deployments designed, for example, to ease customer authentication for online payments in Canada, streamline bank-employee activities in the Middle East, and facilitate regulatory compliance in the European Union. The following maps highlight selected examples of biometrics use in payments and financial services.
5.1 The Americas

In the **United States**, consumers use biometrics for authentication through a number of mobile wallets during debit and credit transactions. Similarly, a growing number of U.S. banks have implemented fingerprint recognition for authenticating account access and financial transactions and are actively exploring other consumer-friendly modalities, including retina-based eye scanning and voice recognition.

Brazil is a world leader in the use of biometrics among consumers, with banks deploying biometric authentication-capable ATMs since 2006. Brazilian banks were responding to widespread opening of fraudulent bank accounts to commit fraud and turned to biometrics to ensure the identities of account holders and protect their accounts. The majority of Brazilian banks now use some form of biometrics to authenticate users, though standards to promote interoperability and wider adoption are lacking.

In 2013, Banco Supervielle, a large bank in Argentina, began installing fingerprint sensors across its network of branches to facilitate the easy and secure transfer of retirement funds to retirees. The new sensors simplified an extensive, complex authentication process that had been instituted to combat fraud (e.g., relatives of retirees receiving pension funds after the death of the retiree).

New payment developments in **Canada** include the use of iris scans and voice recognition to authenticate customers in the mobile space. Another initiative is the Bank of Montreal’s biometric corporate-card program, which allows cardholders to use facial recognition and fingerprint biometrics to authenticate online purchases with greater security and convenience.

Bancolombia’s mobile banking service, Nequi, recently became the first in **Colombia** to deploy mobile biometrics for authentication. The service relies on U.S. fintech company Daon’s IdentityX platform to identify customers through facial-recognition technology. Users authenticate with a selfie when changing devices or SIM cards, resetting passwords, or reactivating an account. The use of biometrics removes friction from the authentication process.

In July 2016, Banco Inbursa announced plans to introduce biometric facial-recognition technology on its mobile banking application and web platform. Banco Inbursa, the first financial institution to offer facial-recognition technology in Mexico, signed a deal to use technology offered by the Spanish facial-recognition solutions provider, FacePhi, which has signed similar deals with banks in other countries – such as Costa Rica, Ecuador, and Guatemala – over the past few years.
5.2 Europe

Dublin, Ireland–startup Touchtech Payments is one of the first technology companies in Europe to develop a solution that utilizes fingerprinting and retinal scanning to authenticate individuals conducting online payments. The company’s technology seeks to help increase online purchase completion rates given that approximately one-third of online transactions are abandoned because users have forgotten their passwords.54

In 2015, ING became the first bank in the Netherlands to introduce voice-activated payments through its mobile banking application, leveraging voice biometrics technology from Nuance Communications.52 With this enhancement, customers can initiate payments using either voice biometrics or fingerprint recognition.

In the United Kingdom, banks are implementing fingerprint recognition, voice recognition, and other biometric authentication solutions on mobile applications. In 2015, Halifax Bank, owned by Lloyds Banking Group, tested the use of a wristband to identify customers by authenticating electrocardiogram (heartbeat) signals.55 HSBC has deployed facial recognition to verify the identity of new account holders; with almost half of all new accounts opened online, the technology allows customers to open an account with a selfie. HSBC expects the process to “become the verification method of choice for its customers.”57

In Russia, the Ministry of Telecom and Mass Communications and the Central Bank of Russia are partnering with Rostelecom to implement the National Biometric Platform (NBP), a pilot project that will allow banks to use biometric identification techniques on clients using a federal information system (the Unified System of Identification and Authentication, or USIA) to verify remote bank-account applications and deliver other banking services.53 To register for remote identification through USIA and NBP, a bank customer visits a branch to undergo the identification process. Once the personal digital profile (including biometric data) is created, the customer will be able to open accounts remotely and access other financial services offered by banks registered with the pilot.

In March 2016, France’s data protection regulatory organization, CNIL, approved La Banque Postale to use a voice biometrics solution by Talk to Pay to authenticate card-not-present transactions for customers. To make an online payment, customers receive an automated phone call in lieu of entering personal information such as name, card number, and expiry date.56 After verifying his or her identity by pronouncing a predetermined sentence, the customer receives a random cryptogram online to finish the transaction. La Banque Postale deployed the program in June 2017.

A number of banks in Germany (e.g., Deutsche Bank and Norisbank) have incorporated Apple’s Touch ID into their mobile banking applications. With Touch ID, customers can gain access to banking services without needing to enter a password.50 Outbank, an independent multi-banking application that supports more than 4,000 banks in Germany, Austria and Switzerland, also offers Touch ID access.51
5.3 Africa and the Middle East

Ghana is in the midst of transforming its banking system to provide access to financial services for the unbanked and the underbanked. To promote financial inclusion, payment-solutions provider Ingenico Group is partnering with a number of local agencies and organizations to extend access using biometric-enabled POS devices; as of summer 2016, some 6,000 terminals had been deployed to enable services such as payments, salary disbursement, cash withdrawals, and bill payment.10

In February 2017, Emirates NBD – a bank based in Dubai, United Arab Emirates – announced a biometric-signature option for customers using specially equipped tablets at branches. The biometric signature aims to more quickly identify customers and thus streamline interactions with bank agents. Bank staff will use the biometric tablets in conjunction with Cockpit, a digital system that allows staff to view customer profiles in a consolidated dashboard.22

In 2016, Standard Chartered announced plans to roll out fingerprint biometric technology to several markets in Africa (Botswana, Ghana, Kenya, Nigeria, Tanzania, Uganda, Zambia, and Zimbabwe).70 Through the Standard Chartered mobile application, clients using touch login can immediately access the bank’s full range of mobile banking services with a registered fingerprint in place of ID and password.

In South Africa, the South African Social Security Agency (SASSA) oversees a biometric grant-disbursement program. The program aims to reduce fraud losses and administration costs and to promote financial inclusion throughout the region. The solution features a biometric-enabled chip card. The cardholder may withdraw the disbursement at SASSA cash pay-points, ATMs, and participating merchant stores.71

In 2016, the Guaranty Trust Bank of Kenya introduced fingerprint authentication to its mobile banking application. Bank executives stated that adding fingerprint recognition was key to providing customers with confidence in the ability to transact securely on its platform. The mobile application also provides customers with secure access to card services, including the ability to check card balances, pay and top up cards, stop card payments, and generate card statements.73
In China, the online payments market has experienced significant growth over the past few years. The rapid adoption of online payments by Chinese consumers has led payments systems – most notably Alipay, Tenpay, and WeChat Pay – to use innovative biometric techniques to provide consumers a secure and uninterrupted user experience. Alipay uses facial recognition, and its parent Alibaba uses biometrics to recognize eye patterns, irises, palm prints, and handwriting.\(^7\)

India’s Aadhaar project provides over 1 billion citizens a unique identification number linked to their fingerprints and iris scans. The project’s objective, to provide “proof of identity” to prevent welfare fraud and promote financial inclusion, is being leveraged to support payments initiatives, including the use of biometrics for authentication of POS and ATM transactions. In April 2017, the government launched Aadhaar Pay for merchants, which can facilitate payments and authenticate Aadhaar-enrolled consumers using a biometric reader at the merchant’s point of sale.\(^8\)

At the end of January 2017, Thailand’s government began rolling out a national e-payment system to reduce the country’s reliance on cash and to support Thailand’s digital-economy policy.\(^7\) Additionally, the Bank of Thailand notified financial institutions that customer password-verification protocols would need to be updated due to increased instances of fraud.\(^8\) In light of these developments and the subsequent increasing demand for secure mobile payments, Samsung launched its biometric-backed Samsung Pay (leveraging fingerprint recognition) in the beginning of February 2017 to enable consumers to purchase items securely with their phones without cash. This was the company’s first Southeast Asian deployment.\(^7\)

The Korea Internet & Security Agency announced in 2017 that it was developing a system for mobile banking authentication using a combination of a fingerprint, heart rate, and electrocardiogram.\(^7\) The biometric authentication technology reads heart rates and electrocardiograms on an individual’s smartwatch and then sends the information to his or her smartphone. The user then unlocks the smartphone with his or her fingerprint, enabling the use of mobile banking.

In Australia, Telstra is experimenting with blockchain technology, combined with facial and voice authentication, to add a layer of security for access to its mobile application.\(^8\) Australia’s government has explored wider use of biometric technology in airports, for visas, and in a new digital identity framework.

In Malaysia, in addition to using biometrics at ATMs, banks are using voice recognition for customer authentication when contacting call centers, alleviating the need for traditional PIN- and security-question protocols and allowing customers to authenticate without any action other than speaking.\(^8\) Customers opt in to the program by recording their voice, with usage expected to save approximately 30 seconds per call.\(^8\)

Banks in Japan have a well-established culture of using biometrics for authenticating customers. The government is testing a biometrics-based payment system that will allow foreign tourists to verify their identity and make purchases during the 2020 Tokyo Olympics.\(^8\) Tourists registering their fingerprints and credit card information will be able to transact without cash or cards at establishments located in tourist locations.

In Japan, the online payments market has experienced significant growth over the past few years. The rapid adoption of online payments by Chinese consumers has led payments systems – most notably Alipay, Tenpay, and WeChat Pay – to use innovative biometric techniques to provide consumers a secure and uninterrupted user experience. Alipay uses facial recognition, and its parent Alibaba uses biometrics to recognize eye patterns, irises, palm prints, and handwriting.\(^7\)

In Australia, Telstra is experimenting with blockchain technology, combined with facial and voice authentication, to add a layer of security for access to its mobile application.\(^8\) Australia’s government has explored wider use of biometric technology in airports, for visas, and in a new digital identity framework.

Customers opt in to the program by recording their voice, with usage expected to save approximately 30 seconds per call.\(^8\)

The Korea Internet & Security Agency announced in 2017 that it was developing a system for mobile banking authentication using a combination of a fingerprint, heart rate, and electrocardiogram.\(^7\) The biometric authentication technology reads heart rates and electrocardiograms on an individual’s smartwatch and then sends the information to his or her smartphone. The user then unlocks the smartphone with his or her fingerprint, enabling the use of mobile banking.
Over the last decade, governments have taken steps to incorporate biometrics into their respective legal frameworks. A common approach has been to apply existing laws covering the collection and sharing of personal data to the context of biometrics. This section provides an overview of the legal landscape in this area.

6.1 Overview of Biometrics-Related Laws

Laws related to biometrics typically revolve around issues of privacy, data protection, and consumer consent and disclosure. Where markets have existing laws covering these issues, some governments have expanded their application to biometric data – for example, adding biometric information to the legal definition of sensitive personal data. Common legal provisions for sensitive personal data include requirements that entities obtain consent before collecting covered data and before sharing that data with a third party. The following chart summarizes select laws and guidance related to biometrics.

<table>
<thead>
<tr>
<th>MARKET</th>
<th>KEY POINTS</th>
<th>DETAILED DESCRIPTION</th>
<th>APPLICABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Voluntary privacy code.</td>
<td>Australia instituted a Biometrics Privacy Code in 2006, with updates in 2015 and 2017. The code was based on privacy standards outlined in Australia’s National Privacy Principles (a section of Australia’s 1988 Privacy Act that regulates the handling of personal information), but also incorporated higher standards of privacy protection, including additional notice obligations and measures to secure the data. The body responsible for developing the Privacy Principles, the Biometrics institute, is a membership organization comprised of government agencies and private companies. The government worked with the institute to revise the code in 2015 and 2017 and provide clarity around implementation responsibilities of the public and private sector, and across Australian state lines.</td>
<td>Companies and government agencies voluntarily sign on to the code. Some companies use the code as a reference point for privacy planning, though the number of signatories has remained low.</td>
</tr>
<tr>
<td>European Union</td>
<td>Current directive does not expressly address biometric data.</td>
<td>The current EU Data Protection Directive (Directive 95/46/EC) framework does not expressly address biometric data and does not include biometrics in the definition of “personal data.” However, the General Data Protection Regulation (GDPR), which takes effect in May 2018, does include a definition of biometric data and includes biometric data in the list of special categories of personal data (i.e., sensitive personal data).</td>
<td>Forthcoming regulation will be applicable to all companies holding data on EU citizens.</td>
</tr>
</tbody>
</table>
### SUMMARY CHART OF SELECT LAWS, REGULATIONS AND GUIDANCE FOCUSED ON BIOMETRICS

<table>
<thead>
<tr>
<th>MARKET</th>
<th>KEY POINTS</th>
<th>DETAILED DESCRIPTION</th>
<th>APPLICABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hong Kong</td>
<td>Government-issued guidance defines biometric data as &quot;personal data.&quot; No formal law distinguishing &quot;sensitive&quot; data from other personal data.</td>
<td>In 2015, the Office of the Privacy Commissioner for Personal Data (PCPD) issued guidance establishing that biometric data should be considered personal data, and that it should only be collected when necessary and not excessively. The guidance states that biometric data should only be collected when there is a clear legal purpose; the collector should conduct an analysis to determine whether biometric technology is essential; data should be secured; and the collector should establish a retention period and delete the data once it is no longer needed for the original purpose. Beyond this guidance, Hong Kong does not have a law formally distinguishing &quot;sensitive&quot; data from other personal data.</td>
<td>Nonbinding, though degree of adherence to the code will be taken into account in any case related to data privacy laws.</td>
</tr>
<tr>
<td>India</td>
<td>Government added rules on &quot;sensitive&quot; personal data to an existing national law.</td>
<td>In 2011, India introduced rules on &quot;sensitive&quot; personal data, including biometrics, to an existing national law called the Information Technology Act, 2000. The rules require that any private or public entity obtain written consent, by fax or email, before collecting &quot;sensitive information&quot;; obtain consent before sharing information with a third party; and establish security practices to secure the data. The rules permit transborder data flows of &quot;sensitive&quot; personal data if: (a) the country to which the data is flowing provides the same level of data protection as India, (b) the transfer is necessary for the performance of a lawful contract between the body corporate or any person acting on its behalf, and (c) consent has been obtained.</td>
<td>Binding for all public and private entities.</td>
</tr>
<tr>
<td>Japan</td>
<td>Government amended an existing law to classify biometric data as &quot;personal identifier code.&quot;</td>
<td>In 2003, Japan adopted a data and privacy law called the Act on the Protection of Personal Information (APPI). In 2015, Japan amended the APPI to specifically classify biometric data as &quot;personal identifier code.&quot; The APPI states that an entity handling personal data, including personal identifier code, must communicate the purpose of collecting the data; keep collected data safe and secure; obtain consent to share the data with a third party (specific consent</td>
<td>Binding for any entity operating in Japan.</td>
</tr>
</tbody>
</table>

The GDPR prohibits the processing of biometric data for the purpose of uniquely identifying a person unless one of 10 exemptions for processing special categories of personal data applies. For example, the processing of biometric data is permitted where the data subject has given explicit consent to the processing. If explicit consent is relied upon, then the GDPR places the burden on the data controller to demonstrate that the consent is: active and freely given; under terms that are easy to understand; simple to withdraw; and provided for each individual processing activity. The GDPR also allows EU member states to introduce further conditions, including limitations, regarding the processing of biometric data. 

Forthcoming regulation (effective May 2018) defines biometrics as "sensitive personal data."
In 2013, South Africa enacted the Protection of Personal Information Act (PoPI), its first law around the protection of personal data. PoPI includes biometrics within its definition of personal data. It requires that any public or private body to obtain permission before collecting personal data and take adequate measures to secure that data. PoPI is modeled after the EU Data Privacy Directive.

At the federal level, the United States does not specifically regulate commercial collection and use of biometric data. Generally, federal law does not require companies that collect such information to follow specific standards for verifying data accuracy; and in most contexts, there is no legal right permitting individuals to correct, amend, or delete incorrect biometric data.

However, the Gramm-Leach-Bliley Act (GLBA) imposes strict privacy requirements on financial institutions with respect to information about their customers. A financial institution is subject to GLBA privacy and data-security requirements when collecting biometric information from a customer in connection with providing a financial product or service. For example, GLBA requires that consumers be provided with notice and an opportunity to opt out when customer information is disclosed to nonaffiliated third parties. GLBA also requires financial institutions to implement an information-security program that includes safeguards appropriate to the institution’s size and complexity, the nature and scope of its activities, and the sensitivity of customer information. As a result, a financial institution would be subject to GLBA privacy and data security requirements when collecting biometric information from a customer in connection with providing a financial product or service to that individual.

A small number of states have laws specifically focused on biometrics (e.g., Illinois, Texas, and Washington). The laws impose limitations or requirements for the collection, use, disclosure and security of biometric information. Other state laws on data privacy and protection may apply to biometric information, though some explicitly state that the statute is inapplicable to a financial institution subject to or in compliance with GLBA.
6.2 Applying Laws to Rapidly Evolving Technologies Such as Biometrics

Biometric technologies are rapidly evolving, with businesses and governments continuing to explore new use cases and applications in the payments environment. Applying existing laws to rapidly evolving technology like biometrics presents unique challenges. The benefits and costs associated with the new technology may change quickly, impacting stakeholders in unexpected ways. Striking a balance between diverse policy objectives – for example, protecting consumer privacy, promoting data security and supporting innovation – may also present challenges. Where laws are implemented, those that are technology agnostic and take a principles-based approach can offer policymakers flexibility as technologies evolve and business models change. Where laws differ across jurisdictions, policymaker coordination can enable an operating environment with more clarity and certainty for both businesses and consumers.

7. Advancing Biometric Authentication: Issues for Further Attention

Biometric authentication is gaining wider acceptance for financial and payment transactions. Although the benefits of speed and convenience are significant, progress toward ubiquitous adoption will require additional effort and focus by a range of payment-system stakeholders. In this section, we describe some of the areas for additional attention, including addressing public-interest concerns around accessibility; developing technology standards to support interoperability; supporting layered, risk-based approaches to payment security; and ensuring the security and privacy of consumers’ personal information.

7.1 Standardization and Interoperability

Standardization of biometric authentication is at an early stage. Standardization can help promote innovation in biometric technologies by making it easier for all parties in the payments ecosystem to adopt and deploy new technologies. Many biometric authentication deployments today operate within a closed-loop environment, in which each manufacturer uses its own proprietary algorithms, scanners, and software. This closed-loop approach ensures that the provider controls the overall user experience, but it also results in limited interoperability for consumers and the absence of a common user experience. If an individual grants a company permission to store biometric data using a proprietary biometric template, the data is not portable and is verifiable only by the technology that computed the biometric template upon enrollment. For example, in 2013 Brazil was among the leading countries globally in deploying biometric-enabled ATMs.
However, the closed-loop nature of the deployments limited customers’ use of the more secure biometric authentication method to ATMs deployed by their own bank. Open, interoperable biometric authentication systems support a common user experience, while enhancing security.

7.2 Layered, Risk-Based Approaches to Payment Security

In the face of an increasingly advanced cyberthreat landscape, biometrics may be most effective when used as part of a layered, risk-based approach to payment security. A risk-based approach allows entities in the payments ecosystem to focus resources and attention on transactions with higher risk profiles, reducing friction at the point of sale and promoting a positive user experience for the vast majority of legitimate transactions. Layering controls can provide enhanced security, as individuals enroll in biometric systems and conduct transactions using biometric authentication.

To mitigate the potential for identity theft and fraud during enrollment in a biometric system, a variety of approaches may be used to ensure that individuals are, in fact, who they say they are and that the linked biometrics are valid. Applying a risk-based approach to enrollment can help to mitigate the risks. For low-risk deployments, self-registration of biometric information may be appropriate. For higher-risk deployments, a more robust biometric enrollment process may be employed involving a review of official identity documents (e.g., government-issued identification) by a human or software trained in this area.

During transactions, authentication processes may take on many forms, with some requiring active involvement of the consumer and others taking place in the background. For example, consumers may be asked to actively provide two credentials to verify their identity. This two-factor approach leverages a secondary credential to mitigate the vulnerability of a single, often static element such as a PIN or password. However, it adds friction to the payment experience and may have a negative impact on completed sales. The growing range of data available on many payment transactions (e.g., device ID, IP address, and geolocation) provides new elements to strengthen authentication in the background, minimizing disruption to the consumer. Many of these data elements can be incorporated into a risk-based analysis of individual transactions, helping institutions focus fraud-mitigation efforts on higher-risk transactions and reducing friction at the point of sale.

7.3 Data Security – Storage and Transmission

A critical decision in implementing and deploying a biometric authentication system is whether the storage and matching of biometric templates take place locally or centrally. The decentralized (or device-based) model enables users to collect and store biometrics on their devices locally. The centralized model involves the collection and storage of biometrics in a central repository, which is used for matching and authenticating access.
In the payments environment, the device-based biometric model has gained popularity (e.g., Touch ID on Apple mobile phones) as it provides a secure way to store biometric data on an individual’s device. With Apple Pay, the biometric data does not leave the device’s operating system; biometric data is not transmitted through the network or through the cloud, making it difficult for hackers to intercept. Centralized storage raises the level of concentration risk, since one successful hack can expose the data of many individuals. For payments, secure solutions that store biometric data in a central database or in the cloud require additional research. Providers are continuing to explore new ways to mitigate risk in the centralized storage model.

New technologies are also being developed to address issues such as biometrics “spoofing.” A spoofing attack occurs when a party pretends to be someone else by falsifying data to gain unauthorized access to that individual’s information. For example, soon after the release of Apple’s Touch ID, hackers figured out how to create dummy fingerprints using Play-Doh to

<table>
<thead>
<tr>
<th>Example</th>
<th>DECENTRALIZED/LOCAL MODEL</th>
<th>CENTRALIZED MODEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advantages</td>
<td>Less attractive as an attack target than a central repository of biometric templates</td>
<td>Potential for increased performance and functionality</td>
</tr>
<tr>
<td></td>
<td>Less biometric data at risk in the event of a successful attack</td>
<td>Re-enrollment not required for each new device</td>
</tr>
<tr>
<td></td>
<td>Does not require the transmission of biometric data</td>
<td>Easier to connect individuals to government programs and benefits</td>
</tr>
<tr>
<td></td>
<td>Supports a higher level of individual choice and control</td>
<td>Potential to identify multiple entries for the same individual (i.e., de-duplication)</td>
</tr>
<tr>
<td>Disadvantages</td>
<td>Lack of software and hardware standardization among different manufacturers</td>
<td>One successful hack can expose the biometric data of many individuals</td>
</tr>
<tr>
<td></td>
<td>Need to re-enroll with each new device</td>
<td>Need to ensure security of data during collection, transmission, and transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elevated privacy concerns regarding security and use, transfer, and sharing of the data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Increased latency (the time the biometric system takes to verify a person's identity)</td>
</tr>
</tbody>
</table>

The advantages and disadvantages of both models are summarized in the table above. Implementing risk management practices and controls that are commensurate with the level and type of risk exposure can help mitigate the risks of either model.
While feasible, biometrics “spoofing” is rare today and not easily scalable. Anti-spoofing measures such as liveness detection, which make it difficult for fraudsters to use a fingerprint copy or a photo to fool biometric sensors, can help to mitigate this risk. A variety of liveness-detection techniques exist, including sensors that detect blood flow or pulse to differentiate spoofed fingerprints from live fingerprints, or cameras that capture 3D structure, micro-movements, or blinking to differentiate between the face of a genuine cardholder and a spoofed facial image of the cardholder.

7.4 Consumer Privacy
Consumers are cautious about giving up personal biometric data, which by nature cannot be replaced if compromised. Although consumers have largely grown comfortable with fingerprint recognition, their comfort with more invasive authentication methods such as iris scanning is not as widespread. As biometrics usage grows in new and varied ways, issues of transparency and consent become more high-profile. Facial-recognition technology, for example, can already be used inconspicuously without knowledge or consent. Behavioral biometrics involving passive participation (e.g., gait recognition without explicit consumer consent) raise questions about consumer privacy. Ensuring that consumer concerns around transparency and consent are addressed will be key to building consumer trust and comfort with biometrics. As outlined in Section 6, a number of governments have begun to incorporate biometrics into existing privacy-related laws.

Government entities collect and store biometric data for a variety of purposes, such as law enforcement. In parallel, organizations focused on consumer privacy, civil liberties and digital rights monitor governments’ ability to use and access biometric information for a variety of purposes, including surveillance, profiling, and criminal prosecutions. Protections against surveillance and government access can be complicated by laws that do not translate simply to modern technology. For example, in the U.S., a Virginia state trial court held that an individual can be legally compelled to unlock a smartphone via fingerprint reader, but not with a passcode. The court reasoned that providing a fingerprint was akin to providing a handwriting sample or an actual key, which the law permits; but a passcode requires the defendant to divulge knowledge, which the law protects against. Providing clear legal frameworks to manage government access to and use of consumer biometrics will help build consumer trust in the technology and its applications in a range of industries.

7.5 Accessibility and Inclusion
Currently, the use of biometrics in most contexts and jurisdictions is voluntary, requiring that consumers opt in to participate. However, a small number of markets are working to implement more universal biometrics programs (e.g., national identity schemes) that link government services to a person’s digital identity.
For certain populations, such as those with physical limitations, biometric systems – which rely on functional physical body parts or traits to complete the authentication process – can impose barriers to essential services. Limitations may stem from physical challenges (e.g., impaired eyes and fingers with limited mobility) or degradation (e.g., worn fingerprints of the elderly or day laborers).

To accommodate users with special needs, policymakers may consider alternatives or fallback options, such as secondary biometric modalities and/or more traditional authentication mechanisms. By addressing these accessibility challenges, policymakers can help ensure that biometric systems serve as inclusive tools to meet policy objectives within their markets.

8 Guiding Principles on Biometric Authentication for Policymakers

The potential for biometric authentication is strong. As policymakers deepen their understanding of biometrics, related technologies, and their implications, they have an opportunity to support the development of this important tool to enhance security in the payments ecosystem. This section provides guiding principles outlining how policymakers can play a critical role in advancing biometric authentication in their markets.

8.1 Foster Stakeholder Dialogue and Engagement

Cross-stakeholder dialogue on evolving technologies such as biometric authentication solutions helps bring a range of voices to discussions that support advancements in the payments ecosystem. Financial institutions, payment networks, industry associations, merchant groups, consumer organizations, regulatory bodies, academics, and think tanks each have unique perspectives to share on payment-system issues, including challenges that require coordination between various parties (e.g., implementation issues regarding deployment, enrollment, data storage, and interoperability).

Engagement may take a number of forms – roundtable discussions, innovation workshops, open comment periods, and other dialogue and feedback mechanisms – to meet the needs of different stakeholders. By fostering dialogue among these groups and engaging in discussions with them, policymakers can deepen their understanding of technology trends, stakeholder perspectives, and potential congruence with policy objectives. Cross-stakeholder discussions may also help build consensus for collective next steps on key issue areas, lessening the need for regulatory action and other government interventions that could negatively impact the long-term development of these rapidly evolving technologies.
8.2 Support Industry-Driven Standards and Interoperability

Standards support payments innovation by making it easier for all parties in the payments ecosystem to adopt and deploy new technologies. By promoting a standards-based approach to authentication, policymakers can help enable all stakeholders in the ecosystem to benefit and participate. Currently, businesses often use proprietary software and hardware in closed systems, limiting interoperability and creating an inconsistent user experience. Open-consensus bodies such as the International Organization for Standardization (ISO), Fast Identity Online (FIDO) Alliance, and EMVCo are currently working to build standards for the biometrics landscape, which is a step in the right direction. Further work by groups like these, in partnership with industry, is necessary to increase interoperability, define security requirements, and provide a consistent framework to evaluate new technology developments.

As technologies advance and connected devices continue to integrate biometric capabilities, it is critical that biometric-authentication policy remains technology-agnostic. Though fingerprinting may be the most common biometric authentication modality used today, we may not be far from wider use of other modalities – physical or behavioral. A policy focus on specific technologies may limit the ability of businesses to invest in new, innovative solutions to meet the rapidly evolving security and cyberthreat landscape. By supporting principles-based standards not tied to a specific technology, policymakers ensure a lasting framework that can keep pace with both innovation and changing risks in the payments landscape.

Interoperability provides the foundation for open and accessible payment systems, creating efficiencies that benefit all ecosystem stakeholders and making it easier to adopt new technologies. In practice, interoperability in the complex payments environment can be challenging to achieve as it requires significant coordination across stakeholder groups. Policymakers can support interoperability by encouraging dialogue and cooperation among the range of payment-system stakeholders involved in developing standards, innovating payment solutions, delivering financial services, and representing others who participate in the payments ecosystem.

8.3 Reframe Security Discussions to Reflect New Technology Developments

Like all burgeoning technologies, biometrics bring both benefits and risks, many of which are discussed in this paper. The institutions that govern such innovation in the payments ecosystem face the constant challenge of keeping pace with technological change and ensuring the security of the payments system without constraining innovation. Historically, many have viewed security and convenience as competing priorities. Biometric authentication, however, presents an opportunity to develop solutions that provide more convenience to consumers while also enhancing security. Many next-generation authentication toolkits are being designed to support a layered approach to payment security with complex verification methods that are difficult for criminals to circumvent. This includes not only
biometrics, but the physical location of the cardholder, IP address, device ID, and other behavioral and contextual data. Many of these methods operate behind the scenes, enhancing security while providing consumers with a more seamless payment experience.

There is no one-size-fits-all solution to payment-system security. Local market conditions – stage of economic development, existing payments infrastructure, and consumer and business preferences about specific modalities – provide important context for discussions about biometric authentication implementation. Risk attributes – such as transaction size, payment channel, and market category – may also influence the appropriate implementation approach. Policymaker guidance that reflects technology developments and evolving security strategies can strengthen payment-system security, allowing ecosystem participants to leverage innovative solutions and approaches to mitigate risk.

8.4 Provide Legal Clarity for Payment-System Participants

Policymakers around the world are starting to promulgate laws and guidance to govern the collection, use, and storage of biometric data, whether explicitly or as part of wider legal responses. This patchwork of laws, along with the lack of interoperable standards, creates uncertainty for ecosystem participants about current and future obligations related to biometric data. This may, in turn, slow user adoption and inhibit innovation.

By engaging in multi-stakeholder discussions on biometric-authentication developments and concerns before the passage of legal measures, policymakers can help build consensus around governance objectives, including assessing whether non-legislative responses – such as industry standards – may be sufficient. Likewise, by providing clarity about legal issues related to biometric authentication – such as data storage, usage, and transmission – policymakers can promote responsible innovation across the industry. Where existing laws differ or conflict between jurisdictions, policymaker coordination can support a more efficient and certain operating environment for entities in the payment system.

8.5 Lead by Example

Policymakers and governments can send a positive message to consumers and businesses alike by embracing biometric technology in their own products and services. Offering biometric-based payment solutions for consumer and business transactions with government – payments for licenses, registrations, taxes, etc. – can enhance security and improve the customer experience. At the local level, governments can incorporate biometric-based payment solutions for services such as public transportation and utilities.
Biometric authentication is experiencing rapid growth and shows great promise across a variety of financial applications in the coming years. Multi-stakeholder dialogue and partnership on solutions that address current challenges can help drive further adoption. However, biometric-authentication adoption across markets will likely be varied, reflecting different market conditions and user preferences. Policymakers play a critical role in cultivating an environment that supports payment-system innovations – not only in the area of biometric authentication, but across the range of authentication and security solutions being developed and tested by ecosystem participants in various markets.
Appendix
Selected Organizations Working on Biometric Issues in Payments

Current efforts to develop global, interoperable standards for biometric authentication are still at a nascent stage. Several organizations are helping to shape the regulatory outlook on biometrics. However, current efforts have not yet led to a common approach in implementation and deployment. Descriptions of these organizations are provided below.

EMVCo

EMVCo aims to facilitate worldwide interoperability and acceptance of secure payment transactions. It manages the evolving EMV Specifications and related testing processes, including card and terminal evaluation, security evaluation, and management of interoperability issues. This work is overseen by EMVCo’s six member organizations – American Express, Discover, JCB, MasterCard, UnionPay, and Visa – and supported by dozens of banks, merchants, processors, vendors, and other industry stakeholders.

In 2016, EMVCo worked to integrate biometrics as a cardholder verification method (CVM), allowing various biometric verification methods to be integrated into the EMV contact payment flow with limited impact on the acceptance infrastructure. The work supports EMVCo’s goal of interoperability by optimizing the existing EMV Integrated Circuit Card Specification for Payment Systems (EMV Chip Specifications) to reduce the impact of implementation. EMVCo is also working with the FIDO Alliance to determine how EMV payment use cases can be incorporated into FIDO Alliance’s technical standards. The focus of this partnership is related to shared cardholder device CVM, for example, using the same biometric method to both open a smartphone and verify a payment made with it.

European Banking Authority (EBA)

The European Banking Authority (EBA) is developing regulatory technical standards on strong customer authentication and secure communication under the second Payment Services Directive (PSD2). Many industry bodies and nongovernmental organizations, such as the FIDO Alliance, were invited to join discussions about how to best promote innovation and improve security on payment transactions, while ensuring consumer protection.

FIDO Alliance

The FIDO Alliance is a nonprofit organization formed in 2012. Its mission is to change the nature of online authentication by setting an open, scalable, and interoperable mechanism that supplants reliance on passwords, in
order to securely authenticate users of online services. FIDO’s primary focus is to develop widely adoptable programs and specifications that can eventually be submitted for formal standardization by recognized standards bodies.

In July 2016, the FIDO Alliance joined efforts with EMVCo on a mobile-payment authentication initiative. The two alliances will collaborate and review how FIDO authentication standards can provide simpler and stronger authentication, such as biometric authentication, for EMV-based payments on mobile devices.

The World Wide Web Consortium (W3C) has also been influenced by FIDO Alliance specifications. The W3C First Public Working Draft, which focused on establishing secure web authentication, was published on May 31, 2016. It represented a landmark for the FIDO Alliance in its mission to spread strong authentication around the globe.

**International Organization for Standardization (ISO)**

The International Organization for Standardization (ISO) is an independent, nongovernmental standardization body with members from more than 163 countries. ISO plays an important role in the standardization of biometrics. The ISO/IEC JTC 1/SC37 working group focuses on standardizing vocabulary, interfaces, interchange standards, and implementation mechanisms. However, these efforts are generally directed towards government applications. The ISO 19092:2008 Financial Services Biometric Security standards describe a framework for using biometrics for authentication of individuals in financial services. In addition, the ISO/IEC 19794 series focuses on global biometric interoperability. Recent work includes the 2016 ISO/IEC TR 30125, which focuses on biometric personalization and authentication in a mobile environment.

**Payments Association of South Africa (PASA)**

South Africa recently changed its specifications to facilitate biometric authentication on payment cards. The new specification was published by the Payments Association of South Africa (PASA) in July 2016 and is designed to allow interoperable solutions on various biometric modalities. Industry players are now able to develop solutions compliant with the standard. This development represents an opportunity for the private sector to deploy biometric authentication in commercial applications.

**U.S. National Institute of Standards and Technology (NIST)**

The U.S. National Institute of Standards and Technology (NIST) has conducted research on biometric modalities for over 60 years. NIST maintains numerous standards and working groups that focus on biometrics. The first standard in biometric authentication was published in 1986 by NIST forerunner the U.S. National Bureau of Standards, on fingerprint use by law enforcement. The ANSI/NIST-ITL standard
covers biometric data interchange in military, law enforcement, disaster management, and intelligence applications, but not use of the data.

U.S. National Science and Technology Council (NSTC)
The White House established the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management (IdM) with the primary objective to advise and assist on policies and procedures. The subcommittee was also tasked with creating plans for federally sponsored biometric and IdM activities. In 2007, the NSTC established a “Policy for Enabling the Development, Adoption and Use of Biometric Standards” in the U.S. This policy consists of a framework to reach interagency consensus on biometric-standards adoption for the federal government.
Endnotes


3 “The end of plastic cards nears: Over 70,000 ATMs will soon support Touch ID withdrawals,” 9to5Mac, July 15, 2016, https://9to5mac.com/2016/07/15/atm-withdrawals-with-iphone-fis-partnership/.


40 "EMV Cards are Proven to Reduce Fraud;" Gemalto, http://www.gemalto.com/emv/fraud/.


66 Kevin Lonergan, “4 things the IoT will make redundant in day-to-day security,” Information Age, October 2, 2015, http://www.information-age.com/4-things-iot-will-make-redundant-day-to-day-security-123490265/.


Marc A. Kowlesko, “Biometric Authentication for Older Adults,” 2012.


About the FIDO Alliance," FIDO Alliance, https://fidoalliance.org/about/overview/.


