PROMONTORY
an IBM Company

Biometric Authentication in Payments

CONSIDERATIONS FOR POLICYMAKERS
Report Summary

November 2017

Prepared by Promontory Financial Group, an IBM Company, for VISA

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, device ID, etc. – available to support new and enhanced authentication services.

Overview of Biometric Authentication

Biometric identifiers (biometrics) are unique, intrinsic physical or behavioral characteristics that can be used to identify or verify the identity of an individual. 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.

Authentication is the process of verifying that an individual or entity is who he or she claims to be. There are three main mechanisms for authentication:

SOMETHING YOU "HAVE"	Something only you possess, like a security token or a smart card
SOMETHING YOU "KNOW"	Something known only to you, such as a password, personal identification number (PIN), or answer to a security question
SOMETHING YOU "ARE"	A personal characteristic that you use to authenticate yourself, such as your fingerprint or iris pattern – *this is the foundation of biometric authentication*

Biometric authentication includes two key phases: enrollment and verification. During enrollment, the individual's biometric data is captured, converted into a template (a coded digital representation of extracted patterns), and stored either locally on a device or

centrally on a server. 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.

In biometric systems, modality refers to the trait used for authentication. Performance, usability, and cost effectiveness of the biometric solution depend on technology maturity and other factors, which vary across modalities. Common types of authentication modalities include: fingerprint, face, iris, palm and finger vein, voice recognition, keystroke, gait, and heartbeat.

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.

The outlook for the use of biometric authentication in payments is positive. 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, risk-based security strategy. Realizing these benefits requires cooperation across stakeholders.

Biometrics Legal Landscape

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. 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.

Applying existing laws to a rapidly evolving technology landscape such as 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, 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.

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.

a. 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. Open, interoperable biometric authentication systems support a common user experience, while enhancing security.

b. 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 as they conduct transactions using biometric authentication. 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.

c. Data Security – Storage and Transmission

A critical decision in implementing and deploying a biometric authentication system is whether the biometric template storage and matching 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 and payment transactions. Each model has advantages and disadvantages. Implementing risk management practices and controls that are commensurate with the level and type of risk exposure can help to mitigate the risks of either model. New technologies are also being developed to address issues such as biometrics spoofing (i.e., when a party falsifies data to gain unauthorized access to an individual's information). Anti-spoofing measures such as liveness detection can help to mitigate this risk.

d. 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. Ensuring that consumer concerns around transparency and consent are addressed will be key to building consumer trust and comfort with biometrics. 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.

e. Accessibility and Inclusion

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. By addressing these accessibility challenges, policymakers can help to ensure that biometric systems serve as inclusive tools to meet policy objectives within their markets.

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.

Guiding Principles on Biometric Authentication for Policymakers

GUIDING PRINCIPLE	DESCRIPTION
1. FOSTER STAKEHOLDER DIALOGUE AND ENGAGEMENT	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.
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. 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.
3. REFRAME SECURITY DISCUSSIONS TO REFLECT NEW TECHNOLOGY DEVELOPMENTS	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.
4. PROVIDE LEGAL CLARITY FOR PAYMENT-SYSTEM PATICIPANTS	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.
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, as appropriate in their market.

Conclusion

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 to 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 also across the range of authentication and security solutions being developed and tested by ecosystem participants across markets.

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