10 August 2020

National Institute of Standards and Technology U.S. Department of Commerce

By electronic mail: dig-comments-RFC@nist.gov

To Whom It May Concern:

Visa appreciates the opportunity to provide input to the National Institute of Standards and Technology (NIST) on Special Publication (SP) 800-63-3 *Digital Identity Guidelines*, SP 800-63A *Enrollment and Identity Proofing*, SP 800-63B *Authentication and Lifecycle Management*, and SP 800-63C *Federation and Assertions* (together, "the Guidelines"). Visa has spent more than 60 years connecting hundreds of millions of people and organizations to a global system that enables fast, safe and reliable financial transactions. However, around the world, 1.7 billion people remain excluded from the formal financial system.[1] Visa envisions a world where all individuals and businesses are able to use secure, convenient, and affordable payment and other financial services to meet everyday needs and long-term goals. Secure digital identity systems can bring more people and more transactions into the formal financial system, thereby encouraging financial inclusion and enabling more financial transparency. In turn, financial inclusion can help put people on a path out of poverty, create productive empowered citizens, foster business opportunities, and fuel economic growth.

The global payments environment is changing rapidly, driven by new technology, emerging competition, and consumer demand for new and innovative services. As the payments ecosystem continues to evolve, policies that support open, secure, and interoperable digital frameworks can facilitate innovative solutions and help drive growth in the digital economy. In our experience, digital frameworks work best when they are principles and risk-based, while ensuring sufficient flexibility to enable innovation.

We provide below our perspective on digital identity and specific observations about the Guidelines, which collectively provide the controls and technical requirements for specified digital identity management assurance levels.

I. INITIAL CONSIDERATIONS ON DIGITAL IDENTITY AND APPLICABLE SERVICES

The need for secure, trusted, and instantly verifiable identities is rapidly growing, as people, businesses, and governments conduct more of their lives and services digitally. In many ways, one's identity and the ability to easily confirm one's identity may impact the types of services, products, and information an individual or business owner can receive. It is an essential tool for commerce and for accessing government and other services in the digital age. This is timelier than ever, as the global COVID-19 pandemic has accelerated digital transformation over recent months.

Specific to the payments ecosystem, Visa believes that secure digital identity systems based on internationally accepted principles can reduce friction for onboarding people and businesses to a financial service or product, allowing for robust consumer due diligence. Digital identity can also improve efficiency and user experience at the moment of transaction or interaction, while

[1] See World Bank Global Findex Database, 2017, available at https://globalfindex.worldbank.org/.

simultaneously improving security and reducing fraud. Especially in light of the ongoing pandemic, digital transformation of our economy can be both a force for economic empowerment on a global scale, or it can exacerbate inequality for those who are unable to participate. Good policy can help embrace this moment to effect positive change for individuals, businesses, and governments alike. Visa is working closely with our ecosystem partners to improve the digital commerce experience for all constituents – from government to businesses and consumers.

II. SPECIFIC OBSERVATIONS ON THE GUIDELINES

Visa commends NIST for providing opportunities for public and private sector collaboration in the development of the Guidelines, as this allows ecosystem players to contribute to the development of the frameworks in which they will participate. We provide below our targeted feedback on the Guidelines for NIST's consideration.

a. Digital identity frameworks must include strong privacy and user right protections

In its request for comment, NIST noted its interest in comments and recommendations on privacy enhancements and considerations. Effective digital identity frameworks depend on trust – earning public trust to enable someone to handle and use important financial and personal data necessitates that entity's commitment to privacy, security, and transparency. Digital identity frameworks should incorporate "privacy by design" principles where user privacy is proactively embedded into the framework.

Visa believes in empowering consumers with tools to easily access, manage, and use their financial information, and supports the progression to strong authentication of consumers who interact with organizations digitally. When presented with an opportunity to enable or access services or information that require consumers to provide their personal data, consumers should receive clear notice as to why they are being asked to provide the requested data and how the data will be used. Consumers should also be offered clear, simple, and consistent information about their choices.

b. Consideration for a phased-out approach from less secure authentication methods

As technology has advanced, authenticator assurance levels have become increasingly important means to ensure robust security measures are in place to protect consumers. While reasonable risk-based assurances are still appropriate for transaction decisions, some approaches, particularly within authenticator assurance level 1, are quickly becoming outdated and may pose a greater risk of data security breaches, thus eroding consumer trust. To ensure the continued safety and security of the payments ecosystem, Visa believes less secure authentication methods, such as passwords or memorized secrets, single SMS OTP, and other vulnerable authenticator types, should be phased out over time or complemented with other secure mechanisms. We recognize that phasing out existing technologies in a non-disruptive way will take some time and require coordinated industry efforts. We also note that risk-based assessments may be a helpful tool to best determine the ways in which authentication is performed.

c. Request for additional specifications on identity assurance levels

Different identity assurance levels are required to support robust enrollment and identity proofing. As the process for providing identity documentation increasingly moves from a physical environment to a digital one, we request that NIST revise the identity assurance levels to account for primarily remote

and other digitized methods so that providers can efficiently and securely support changes in technology and consumer behavior. Additionally, the increased adoption of digital forms of identity (*e.g.,* mobile driver's licenses, eIDs), should be factored into assurance level requirements to ensure appropriate support for these technologies. Visa supports the standardization of online identity proofing currently undertaken by the FIDO Alliance Identity Verification and Binding Working Group.

d. Application of the Guidelines to federated and decentralized digital identity models

Over the past several years, new forms of digital identity models have emerged, with model requirements often varying widely. Federated identity models, where several entities (perhaps through a particular framework) let subscribers use the same identity data to obtain access to the networks of all of the enterprises in the group, are being widely adopted, as open banking and other data-sharing services proliferate. Under decentralized identity models, ultimate control of identity data sits with the user, thus shifting even further from traditional identity management approaches. As these models continue to gain traction and widespread adoption, it is important to understand their place within existing digital identity guidelines. To this end, we request that NIST provide guidance on the ways in which the Guidelines should be applied to federated and decentralized identity models.

e. Consideration for consumer activities

At Visa, our commitment to the consumer is paramount and the primary consideration for data-driven activities. A successful digital identity framework should encourage innovation, enhance consumer convenience, and empower consumers to manage their data, while protecting consumer privacy and data security. We welcome information in the Guidance about how consumers should understand and engage with their data privacy and data security rights, and the role of managed consumer permissions in the digital identity ecosystem. Consumer trust is essential to the successful adoption of any product or system. In order to best ensure a smooth transition from physical to digital identity systems, consumers must understand the benefits of digital identity and the safeguards in place to protect their financial and personal data.

As financial technology evolves, we recognize the importance of secure, trusted, and verifiable digital identities. Visa appreciates the opportunity to provide our perspectives on SP 800-63-3 *Digital Identity Guidelines*, SP 800-63A *Enrollment and Identity Proofing*, SP 800-63B *Authentication and Lifecycle Management*, and SP 800-63C *Federation and Assertions*. We look forward to working with NIST to continue to refine this framework and welcome additional opportunities to engage in this important work.

Sincerely

David Henstock .