Comments of the World Privacy Forum to the Board of Governors, Federal Reserve

Regarding

Debit Card Interchange Fees and Routing, 86 FR 26189, Docket No. R-1748, RIN 7100-AG15

Via email to: regs.comments@federalreserve.gov

Ann E. Misback, Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

August 11, 2021

The World Privacy Forum appreciates the opportunity to provide comments regarding *Debit Card Interchange Fees and Routing*, 86 FR 26189, Docket No. R-1748, RIN 7100-AG15. https://www.federalregister.gov/documents/2021/05/13/2021-10013/debit-card-interchange-fees-and-routing. The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, including financial privacy. We publish a large body of privacy information, including public comments, research, and work directed to consumers. We testify before Congress and federal agencies on topics related to the financial sector, most recently the Senate Banking Committee, and we submit comments on financial sector regulations. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

The Dodd-Frank Act of 2010 created meaningful improvements for consumers, some of which also improved certain privacy interests of consumers. Now, more than a decade later, technology has advanced, and regulatory updates are needed. WPF finds that many of the changes the Board of Governors of the Federal Reserve System have proposed in its update of Regulation II to be beneficial. We do, however, note some issues that need further attention, particularly regarding authentication and biometrics in the debit card payments context, which we discuss below. The discussion below pertains to *Comment 235.7 (A)-1, Scope of Restriction.*

I. Issues relating to biometrics and payment systems authentication (*Comment 235.7 (A)-1, Scope of Restriction*)

The Federal Register notice (Appendix A to Part 235) states in part:

> The Board proposes to update the examples of cardholder authentication methods listed in the commentary to better align with current industry practices. The proposed revisions add biometrics to the list of cardholder authentication methods in the commentary, which currently only includes signature and PIN authentication.

A. We support the proposed changes to the scope of restriction language, understanding that biometric authentication is already used in the payments marketplace.[1] However, to date, biometric authentication itself for debit cards and related payment systems has not been fully addressed in terms of Federal financial sector regulations. There is important work to be done here — biometric authentication requires additional constraints and rules in the form of quality control measures.

B. Biometric authentication used in the debit card / payments context needs to be required to be provably accurate and provably unbiased, based on independent testing. Biometric software and hardware systems selected to be used for authentication for debit cards or digital wallets (or other methods) need to undergo testing by NIST or another independent body. Baseline parameters of acceptable accuracy and efficacy ranges for biometric systems need to be established. For example, a biometric system utilized for card payment authentication purposes should be able to demonstrate that it operates with provably low to no problems with accuracy or bias, including race, age, gender, and ADA, among other values, such as resilience against fraud.

We acknowledge that this is a large issue area, and to put it colloquially, this line of inquiry regarding biometric authentication opens a can of worms. However, biometric authentication is already used in the marketplace. And NIST testing has demonstrated that biometric system quality varies significantly. Decades of NIST testing has documented in detail the ways that biometric systems differ widely in algorithmic quality, speed, accuracy, the potential for bias regarding age, gender, and race, and in firmware / hardware quality, among others.[2]

For example, from NIST we know that some biometric hardware-software combinations (certain fingerprint systems, for example) have demonstrated extremely low levels of error. New pandemic-era work is underway at NIST regarding contactless fingerprints. Contactless fingerprints are undergoing rapid improvements, however, contactless fingerprints are generally not yet as accurate as those requiring contact.[3] Rigorous testing and publication of results needs to be the norm for any authentication method utilized, including biometrics. We request that the Board of Governors encourage such testing and publication.

C. In debit card payments systems, it is important to ensure that reliable, auditable quality control mechanisms and benchmarking values are in place for authentication technologies — including biometrics. Authentication policies do not always move as quickly

---

[1] We note that Apple iPhones utilize various forms of biometric authentication integrated with the Apple Pay digital wallet: https://www.apple.com/apple-pay/ . MasterCard has a biometric payment card system: https://www.mastercard.us/content/dam/mccom/en-us/documents/biometric-card-merchant-faq.pdf. Visa has been piloting a biometric card: https://usa.visa.com/visa-everywhere/security/biometric-payment-card.html.

[2] NIST, *Biometrics*. https://www.nist.gov/programs-projects/biometrics.

[3] *CRADA Program: Contactless fingerprint capture device measurement*, NIST, ongoing. https://www.nist.gov/itl/iad/image-group/crada-program-contactless-fingerprint-capture-device-measurement .

as the technology. However, problems associated with sophisticated data breaches have created incentives for increased attention and work in the area of authentication. At least one authentication technology — biometrics authentication — is new enough that it lacks sufficient guidance and quality control mechanisms, as discussed previously. In the financial sector, and specifically in the context of debit payment cards, it is important for the Board of Governors to determine the parameters of what quality assurances should be required in a debit payment system, what the acceptable cut-off levels are for the system, and what consumers should be required to be informed of regarding efficacy, accuracy, safety, among others. How accurate, exactly, must a biometric system be? This is something that we would like to see as part of the discussion.

For consumers who are utilizing biometric debit cards, accuracy cut-offs and tests for multiple measures (age, race, gender biases, more) are important quality assurance mechanisms. Consumers using biometric debit cards, Apple iPay, or other systems utilizing biometrics are unlikely to be technical experts in the field. Even with expertise, consumers would still need the industry to conduct and publish benchmark testing on a regular basis to make proper determinations about the trustworthiness of such systems. And those benchmarks would need to be consistent across the payments sector.

The financial sector and consumers would benefit from further guidance that creates requirements and specifications for quality control in biometrics used in debit card systems for authentication purposes. Guidance would ideally ensure that the technology is required to produce results that are consistent with existing financial sector regulations, including the protection of vulnerable classes, as described in the Equal Credit Opportunity Act.

We note that biometrics is an issue area of high interest to consumers, and there are numerous consumer concerns regarding privacy, fairness, and additional matters. A simple web search will collect a high volume of consumer opinion, news reports, academic studies, and government studies regarding biometrics and their use. We observe a disconnect here between consumer interest in and concern about some biometric systems, and a lack of financial sector guidance and transparency to consumers regarding the quality of its biometric authentication systems in terms of accuracy, efficacy, the potential for bias, privacy, and other measures.

II. Issues relating to "future proofing" authentication system guidance (*Comment 235.7 (A)-1, Scope of Restriction*)

Comment 235.7 (A)-1, Scope of Restriction (Appendix A to Part 235) states in part:

> The Board further proposes adding "or any other method of cardholder authentication that may be developed in the future" to capture cardholder authentication methods that do not yet exist and that would still be captured by Regulation II if they were to be developed.

D. Cardholder authentication is of high importance, and we support the inclusion of future-proofing language regarding cardholder authentication methods.

E. Regarding methods of cardholder authentication that may be developed in the future, it is important to set measurement requirements and quality standards. It is crucial that guidance is available that includes the idea that future authentication method(s) need to be quantified in terms of accuracy, efficacy, and fairness, and that the quality statistics regarding the authentication method be made transparent and readily available to regulators and

consumers. A process of ongoing testing should be required to ensure fairness and efficacy of new authentication technologies, and to ensure that new methods are fair and unbiased.

We request that the updated Federal Financial Institutions Examination Council, *Authentication and Access to Financial Institution Services and Systems* (August 2021) is considered in thinking about biometrics and overall authentication issues, including future proofing. We note that in its 2021 guidance, the FFIEC prominently mentions several aspects of biometrics, including behavioral biometrics, as authentication solutions.[4]

III. Conclusion

We support the updated language that is proposed in *Comment 235.7 (A)-1, Scope of Restriction*, with the understanding that more needs to be done in determining and setting quality assurance measures for authentication methods in general, and for biometric methods in particular.

WPF understands that it is important to include biometrics in the list of cardholder authentication mechanisms. Because biometrics has become important as a financial sector authentication method, it will be important to set procedures to ensure fairness and quality in such systems.

Given the new inclusion of biometrics in the *Scope of Restriction,* we request that the Governor's Board undertakes an analysis of what it could do, or could be done, to create standards and quality assurance mechanisms in this area. It is in our collective best interest to ensure the highest possible quality, efficacy, and fairness of all debit card authentication systems.

We would welcome the opportunity to discuss this further.

Respectfully submitted,

Pam Dixon

Executive Director,
World Privacy Forum

[4] August 2021. https://files.consumerfinance.gov/f/documents/cfpb_authentication-access-financial-institution-services-systems_guidance_2021-08.pdf