

MasterCard Worldwide  
Law Department  
2000 Purchase Street  
Purchase, NY 10577-2509  
tel 1-914-249-2000  
www.mastercard.com



October 28, 2016

*Via Web-Based Submission*

Federal Trade Commission  
Office of the Secretary  
Constitution Center  
400 7th Street, S.W., 5th Floor, Suite 5610 (Annex B)  
Washington, DC 20024

**RE: Safeguards Rule, 16 CFR 314, Project No. P145407**

Dear Secretary Clark:

MasterCard International Incorporated (“Mastercard”) submits this comment letter to the Federal Trade Commission (the “FTC”) in response to its request for public comment on its Standards for Safeguarding Customer Information (the “Request for Comments”).<sup>1</sup>

Mastercard appreciates the opportunity to provide input on the Request for Comments. We generally believe that there is no reason for the FTC to revise its Standards for Safeguarding Customer Information<sup>2</sup> (the “Safeguards Rule”) to provide more specific requirements or to incorporate other information security standards or frameworks.

***Background on Mastercard***

Mastercard is a technology company in the global payments industry. We operate the world’s fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard’s products and solutions make everyday commerce activities—such as shopping, traveling, running a business and managing finances—easier, more secure and more efficient for everyone.

Mastercard does not issue credit cards or other payment cards of any type, nor does it contract with merchants to accept those cards. In the Mastercard payment system, those functions are performed in the United States by numerous depository institutions. Mastercard refers to the depository institutions that issue payment cards bearing the Mastercard brands as

---

<sup>1</sup> 81 *Fed. Reg.* 61,632 (Sept. 7, 2016).

<sup>2</sup> 16 C.F.R. § 314.3.

“issuers.” Mastercard refers to the depository institutions that enter into contracts with merchants to accept Mastercard-branded payment cards as “acquirers.” Mastercard owns the Mastercard family of brands and licenses depository institutions in the United States to use those brands in conducting payment transactions. Mastercard also provides the networks through which its customer depository institutions can interact to complete payment transactions and sets certain rules regarding those interactions.

When a cardholder presents a Mastercard-branded payment card to a merchant to purchase goods or services, the merchant sends an authorization request to its acquirer, the acquirer routes the request to Mastercard, and Mastercard routes the request to the issuer. The issuer either approves or declines the authorization request and routes its decision back to the merchant through the same channels. Mastercard’s role in the transaction is to facilitate the payment instructions between the parties to the transaction—the cardholder, the merchant, the acquirer, and the issuer. In an automated teller machine (“ATM”) transaction, Mastercard similarly transmits instructions between the ATM operator and the issuer.

### ***Feedback on the Request for Comments***

Mastercard believes the FTC’s Safeguards Rule has played an active role in balancing access to personal information for legitimate purposes while ensuring security of such personal information. We would like to focus our comments on three questions posed by the FTC in the Request for Comments: those set forth in Sections B.1, B.2 and B.3 of the Specific Issues for Comment.

*B.1. Should the elements of an information security program include a response plan in the event of a breach that affects the security, integrity, or confidentiality of customer information?*

Mastercard believes it is not necessary to modify the elements of an information security program to include a response plan in the event of such a breach. The Safeguards Rule already requires covered entities to implement and maintain an information security program that is appropriate to their size and complexity, the nature and scope of their activities, and the sensitivity of any customer information at issue. As such, entities for which it is appropriate to have a response plan should implement and maintain one under this standard.

As the FTC stated in the commentary when it adopted the Safeguards Rule, the current standard is highly flexible, consistent with the comments the FTC received on the Advanced Notice of Proposed Rulemaking, consistent with the guidelines issued by the federal banking agencies at the time, and consistent with the recommendations in the report issued by the FTC’s own Advisory Committee on Online Access and Security.<sup>3</sup> Moreover, the characterization of the FTC’s position was recently reiterated by the FTC’s staff: “the touchstone of the FTC’s approach to data security has been reasonableness—that is, a company’s data security measures must be reasonable in light of the volume and sensitivity of information the company holds, the size and

---

<sup>3</sup> 67 Fed. Reg. 36,484, 36,488 (May 23, 2002).

complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors."<sup>4</sup>

The FTC's position is well known. The existing Safeguards Rule has created the boundaries within which companies must develop reasonable information security programs. The Safeguards Rule allows companies to make informed, risk-based decisions about the resources they dedicate to their information security program without having to allocate additional resources to aspects of a program that may not be necessary or appropriate for their own situations. Additionally, companies like ours that provide services to depository institutions, not consumers, already are subject to breach incident requirements under agreements with those depository institutions.<sup>5</sup> The bottom line is that the Safeguards Rule has worked well in its current form, and we are not aware of any reason that the FTC should change it to require a response plan.

*B.2 Should the Rule be modified to include more specific and prescriptive requirements for information security plans?*

For the same reasons that we do not believe that the information security program should include a response plan requirement, we do not believe that the Safeguards Rule should include more specific and prescriptive requirements for information security plans.

*B.3 Should the Rule be modified to reference or incorporate any other information security standards or frameworks, such as the National Institute of Standards and Technology's Cybersecurity Framework or the Payment Card Industry Data Security Standards?*

Mastercard does not believe the FTC should incorporate any other information security standards or frameworks into the Safeguards Rule. Mastercard co-founded and developed the Payment Card Industry Data Security Standards ("PCI DSS") in 2006. The PCI DSS are an essential part of securing the payments ecosystem, which is why we mandate compliance with PCI DSS for participants in our network. The PCI DSS are unique in that they were developed by the major card networks and apply specifically to participants in the card industry. Whereas the PCI DSS may be appropriate for payment card issuers and acquirers, for example, they would not necessarily apply to all FTC-supervised financial institutions.

Importantly, the PCI DSS differ from the Cybersecurity Framework developed by the National Institute of Standards and Technology (the "Framework"). The latter was designed to apply more generally to "critical infrastructure"<sup>6</sup> but also on a voluntary basis to help

---

<sup>4</sup> Arias, Andrea, *The NIST Cybersecurity Framework and the FTC* (Aug. 31, 2016).

<sup>5</sup> Interagency guidance obligations depository institutions to develop response programs that include service provider controls. See Supplement A to Appendix B to 12 C.F.R. Part 30 (Office of the Comptroller of the Currency), Appendix F to 12 C.F.R. Part 225 (Board of Governors of the Federal Reserve System), and Appendix B to 12 C.F.R. Part 364 (Federal Deposit Insurance Corporation).

<sup>6</sup> "Critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Exec. Order No. 13636, 78 *Fed. Reg.* 11,739 (Feb. 19, 2013).

organizations manage cybersecurity risk.<sup>7</sup> The Framework is not designed to replace an organization's cybersecurity risk management.<sup>8</sup> Rather, an organization can use the Framework as part of its systematic process for identifying, assessing and managing cybersecurity risk. Even the FTC staff has stated that the Framework "is not, and isn't intended to be, a standard or checklist" and that "there's really no such thing as 'complying with the Framework.'"<sup>9</sup>

We believe that the FTC should continue to recognize that the Framework is not a binding set of obligations upon organizations. Indeed, the Framework is intended primarily to assist critical infrastructure. While the Department of Homeland Security has designated the financial services sector as a critical infrastructure sector, the Framework would surely not apply to all financial institutions over which the FTC has authority. While the Framework may represent a risk-based approach to managing cybersecurity, any reference in the Safeguards Rule to the Framework or to any other information security standards could suggest mandatory compliance. This is inconsistent with the purposes for which the Framework was developed and how it has been treated by industry. Therefore, Mastercard encourages the FTC not to incorporate or reference any information security standards or frameworks in the Safeguards Rule.

\* \* \*

Again, Mastercard appreciates the opportunity to provide comments on the Proposed Guidance. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at (914) 249-6715 or [Randi.Adelstein@mastercard.com](mailto:Randi.Adelstein@mastercard.com), or our counsel at Sidley Austin LLP in this matter, Joel D. Feinberg, at

Sincerely,

Randi D. Adelstein  
Assistant General Counsel, Regulatory Affairs

cc: Joel D. Feinberg

---

<sup>7</sup> National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* 1 (Feb. 12, 2014).

<sup>8</sup> *Id.* at 4.

<sup>9</sup> Arias, *supra* note 5.