



November 7, 2016

Submitted Electronically via www.regulations.gov

Mr. David Lincicum and Ms. Katherine McCarron
Division of Privacy and Identity Protection, Bureau of Consumer Protection
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave. NW
Suite CC-5610 (Annex B)
Washington, DC 20580

RE: Safeguards Rule, 16 CFR 314, Matter No. P145407

Mr. Lincicum and Ms. McCarron:

The National Retail Federation (NRF) is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

We appreciate the opportunity to comment on the Standards for Safeguarding Customer Information (the "Safeguards Rule") as part of the systematic review by the Federal Trade Commission (FTC) of its rules and guides. Please note, however, the comments herein provide our views on only one, discreet section of your request for public comment – the incorporation of information security standards into the Safeguards Rule – and the absence of comments on other aspects of your inquiry should not be construed by the Commission or other parties as support for the FTC's position.

In section III.B.3. of the FTC's September 7, 2016 request for public comment on the Safeguards Rule, the Commission specifically inquired whether the Safeguards Rule should be "modified to reference or incorporate any other information security standards or frameworks, such as the...Payment Card Industry Data Security Standards."¹

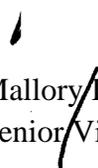
We urge the FTC *not* to rely on Payment Card Industry Data Security Standards (PCI DSS) for any purpose, particularly not for reference or incorporation in its Safeguards Rule, nor for any determination of industry best practices or what may constitute reasonable data security standards in the payment system or any other sector. To address the Commission's specific questions in section

¹ *Standards for Safeguarding Customer Information*, 81 Fed. Reg. 61,632, 61,635 (Sept. 7, 2016).

III.B.3, we have attached and include as part of these comments a white paper that details our standard-setting and competition policy concerns with PCI. As a proprietary organization formed and controlled by a single industry sector (i.e., the major credit card networks), PCI is not an open organization built on standard-setting principles recognized by the United States Standards Strategy (published by the American National Standards Institute, better known as ANSI). Notably, PCI fails to satisfy *any* of the principles adopted by the federal government for voluntary standard-setting organizations that are intended to promote sound, fair standards and avoid the competition problems that can be inherent in any standard-setting process that is not carefully constructed.

For the reasons discussed in the attached analysis, we encourage you to investigate PCI's processes and practices, and not reference or incorporate them in the Safeguards Rule. We believe you will conclude that PCI itself is an inappropriate exercise of market power by the dominant U.S. payment card networks and PCI should not set industry data security standards through its current processes. Furthermore, the Commission should not allow PCI, a self-interested private entity, to substitute its judgment for that of the Commission with respect to the substance of the Safeguards Rule. Not only would this entrench the monopoly positions of the large card networks, but it would put the government's imprimatur on PCI DSS and effectively grant this closely-controlled, private entity the regulatory power of the government itself.

Sin


Mallory B. Duncan
Senior Vice President and General Counsel

Attachment:

PCI Data Security Standards: Federal Standard-Setting and Competition Policy Concerns

cc: Hon. John Thune, Chairman, U.S. Senate Commerce Committee
Hon. Bill Nelson, Ranking Member, U.S. Senate Commerce Committee
Hon. Fred Upton, Chairman, U.S. House Energy and Commerce Committee
Hon. Frank Pallone, Ranking Member, U.S. House Energy and Commerce Committee

PCI DATA SECURITY STANDARDS: FEDERAL STANDARD-SETTING AND COMPETITION POLICY CONCERNS

EXECUTIVE SUMMARY

As part of its effort to ensure businesses are implementing reasonable data security practices, the Federal Trade Commission (“FTC”) is gathering information about the functioning of Payment Card Industry Data Security Standards (“PCI DSS”). However, the Payment Card Industry Security Standards Council (PCI), which develops and maintains PCI DSS, does not follow the standard-setting principles approved and recognized by the FTC, the broader set of U.S. government agencies, or members of the World Trade Organization’s Technical Barriers to Trade Agreement.

Accepted standards development principles include: transparency, openness of participation, impartiality, effectiveness, consensus-based decision making, and due process, among others. Congress and federal agencies, through the Standards Development Organization Advancement Act and related guidance, have formally adopted similar principles to identify the types of voluntary standard-setting bodies that may be relied upon by the federal government. PCI does not satisfy *any* of these principles.

PCI is not an open organization built on consensus or maximizing results. PCI is a proprietary organization formed and controlled by a single industry sector—the major card networks (e.g., Visa, MasterCard)—with motivations that conflict with the interests of businesses and consumers who use the payment card system, including retailers and their customers.

Further, PCI’s standards are not voluntary. Instead, they are set by networks with market power and are forced upon business owners (and, by extension, their customers) that cannot refuse to accept credit and debit cards. PCI effectively stifles competition and innovation by consuming funds otherwise available for data security, and for adoption and implementation of new—possibly more secure—payment technologies.

The card networks, in other words, unfairly leverage their brands and proprietary technology through webs of closely-controlled interdependent bodies and compliance regimes. PCI is very much a part of this overall anticompetitive scheme. The FTC should be very wary of the nature of PCI and the effects of its standards and processes. Ultimately, PCI is a mechanism through which the payment card networks that control it unfairly leverage their market power.

PCI DSS should not be viewed as standards that may be voluntarily adopted by card-accepting businesses. They are the converse – they are involuntary. PCI mandates data security requirements for other businesses; it is not an open standard-setting body that proposes voluntary self-regulatory guidance. Government should not embed PCI’s privately-controlled mandates into its legal determination of reasonable data security practices. Not only would this entrench the monopoly positions of the large card networks, but it would put the government’s imprimatur

on PCI DSS and effectively grant this closely-controlled, private entity the regulatory power of the government itself.

For all of the reasons discussed herein, PCI DSS should not be relied upon by any U.S. government agency, including the FTC, as indicia of an open, competitive industry standard for reasonable data security. We urge the FTC to:

- Investigate PCI's processes to determine whether those processes meet the requirements for standard-setting laid out by federal law and policy.
- Investigate the PCI standards and how those standards are implemented and enforced by the payment card networks that control PCI in order to determine whether the standards and their implementation violate competition laws.
- Reject the use of PCI DSS as a benchmark for reasonable data security practices in light of the facial problems with PCI's processes and standards.
- Work with legitimate standards bodies to ensure that standards for the payment card industry and card security are set in a manner that is consistent with the United States Standards Strategy and U.S. competition policy.

In the discussion below, this paper provides a more detailed description of PCI, including its history with the retail industry and its governance structure, functions and enforcement activities. We also include a discussion of U.S. government-accepted principles for standards development and voluntary standard-setting bodies, and the ways in which PCI fails to satisfy those principles. The paper concludes with an analysis of PCI's apparent conflicts of interest and misaligned incentives vis-à-vis other industry participants and consumers.

DISCUSSION OF STANDARD-SETTING AND COMPETITION POLICY CONCERNS

Under authority granted to it by Congress in Section 5 of the Federal Trade Commission Act, the FTC requires businesses to use reasonable data security practices to protect sensitive consumer information or face administrative enforcement actions for unfair or deceptive acts or practices.

Currently, the FTC is gathering information about the functioning of PCI DSS for card-accepting businesses. However, the FTC has not, to date, critically evaluated the structure or membership of PCI, the proprietary nature of PCI DSS requirements (and their effects on other businesses), or the significant anti-competition and conflict-of-interest problems associated with PCI DSS. These concerns should be taken into account by the FTC in assessing the appropriateness of using PCI DSS as a foundation for what constitutes reasonable data security practices.

The following discussion provides a detailed description of PCI's history, structure and processes, and the standard-setting and competition problems in the payment card system created by PCI DSS. It concludes with a set of recommendations for the FTC's consideration in determining how best to address these significant concerns.

I. Background on PCI

A. National Retail Federation History with PCI

The National Retail Federation ("NRF") has a longstanding history with the card networks' data security initiatives. Around 2003, Visa approached NRF with a proposal to impose Visa's proprietary data security system ("Cardholder Information Security Program" or "CISP") on brick-and-mortar retailers for in-store transactions. NRF members balked at Visa's plan largely because of concerns that the other card networks (e.g., MasterCard, JCB International) would also attempt to unilaterally impose their own—possibly different and conflicting—security standards on retailers. Complying with several involuntary proprietary data security regimes was considered infeasible and cost-prohibitive, and was vigorously opposed by NRF's members.

Further, NRF suspected that Visa (followed by the other card networks) was attempting to shift the cost burden and liability for the data security of an increasingly antiquated and fraud-prone card system onto retailers, even though the networks and card-issuing banks controlled, as they do now, the security features on cards (e.g., magnetic stripes on cards, card numbers embossed on the front of cards, use of static account numbers to access value, availability or non-availability of PINs associated with cards, etc.). When discussing its proposed imposition of CISP with NRF and its members, Visa also showed (as it still does) an unwillingness to consider security measures that placed costs or burdens on the networks or card-issuing banks. Instead, Visa was only willing to discuss some measures that impacted *retailer* and acquiring-bank obligations. Finally, it was clear that Visa's proposal had been developed without any significant consideration of retailers' business operations or ripple effects on other card brand acceptance. All of this fueled NRF's apprehensions about, and strong opposition, to Visa's plan.

In apparent response, at least in part, to NRF's concerns, Visa proposed the creation of PCI. While the stated purpose of the organization was to bring "independence" to the security standards process, instead it brought to fruition retailers' concerns about cost and compliance burdens and the shifting of those burdens away from card networks and banks onto card-accepting merchants.²

B. PCI Creation

PCI was created in 2006 by the major credit card networks to develop and implement security standards for the payment card industry.³ PCI's founding members include American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. (collectively, the "networks"). To effectuate PCI's standard-setting activities, the networks incorporated PCI DSS into their respective data security compliance programs (i.e., mandatory operating rules governing the issuance and acceptance of payment cards branded with their logos).

C. Current Leadership and Organizational Structure of PCI

PCI is currently governed by an Executive Committee comprised of the five founding networks.⁴ The networks share equally in governance and execution of PCI's work. "Strategic Members" of PCI are also eligible to participate on the Executive Committee. The Strategic Membership level is open to "multinational acceptance marks [(i.e., other card brands)] with demonstrated commitment to PCI Security Standards."⁵ There are no Strategic Members of PCI at this time. Thus, the organization is governed exclusively by the five founding card networks. Visa and

² Visa and MasterCard each individually have market power sufficient to unilaterally impose requirements on retailers; by extension, a group of the major card networks like those that run PCI has the power to impose such involuntary standards. *See U.S. v. Visa*, 344 F.3d 229, 239 (2d Cir. 2003) ("Visa and MasterCard, jointly and separately, have power within the market for network services.").

³ As discussed in more detail above, creation of PCI followed an unsuccessful attempt by Visa to impose on brick-and-mortar retailers its own proprietary CISP program for in-store sales. When retailers balked at Visa's plan, Visa moved to create a purportedly "independent" group to establish and impose data security requirements on merchants, but PCI was comprised of only Visa and the other major card networks who control its operations and enforce its requirements.

⁴ Unless otherwise noted, all background information on PCI is taken from the organization's public website at www.pcisecuritystandards.org.

⁵ "Acceptance marks" generally refer to logos (i.e., brand names like Visa, MasterCard, Diners Club, Discover, etc.) that signify which types of cards are accepted at a given location. China's UnionPay is an example of a multinational acceptance mark.

MasterCard each, individually, have market power in the credit card market⁶ and, therefore, the payment card networks controlling PCI clearly have market power as a group.

In addition to the Executive Committee, PCI has a Standards Committee and an Operations Committee. The Standards Committee maintains PCI's security standards and all other technical work product, and develops and manages working groups, special interest groups and task forces on all technical matters. The Operations Committee manages PCI's day-to-day functions and provides guidance to the Executive Committee on corporate and operational matters.

Membership on the Standards Committee and the Operations Committee is limited to the founding networks, Strategic Members, and PCI employees. Again, because there are no Strategic Members of PCI at this time, the founding networks have exclusive control over these committees and their activities.

Other membership categories (aside from Strategic Members) in PCI include: Participating Organizations, a Board of Advisors, an Affiliate Class, and Special Interest Groups. Their respective eligibility parameters and roles are as follows:

- **Participating Organizations** include entities affiliated with the payment card industry (e.g., banks, processors, hardware and software developers, merchants, and point-of-sale vendors). Participating Organizations pay annual dues (\$3,500) and are provided with the opportunity to review security standards in advance of their release and to comment directly to PCI prior to release. Further, Participating Organizations get access to certain PCI communications and webinars, and may contribute to the PCI blog. Participating Organizations *do not* serve on PCI committees and are not involved in setting PCI's security standards.⁷
- **Board of Advisors** members are cross-industry representatives of the Participating Organizations. They "provide input to the organization and feedback on the evolution of the PCI standards." Board of Advisors members also *do not* serve on PCI committees.
- **Affiliate Class** members are "regional and national organizations that define standards and influence adoption by their constituents who process, store, or transmit cardholder data." These members may serve on working groups, which are controlled and managed by PCI's Standards Committee (i.e., the founding networks).

⁶ See *U.S. v. Visa*, 344 F.3d at 239.

⁷ Participating Organizations merely have the opportunity to offer non-binding comments to the organization after standards are developed.

- **Special Interest Groups** are formed to analyze and address specific industry or technological challenges, and propose changes, clarifications or improvements to PCI standards and programs. These groups are overseen by the Standards Committee (i.e., the founding networks).

Retailers—through NRF and others—have made repeated requests to participate on PCI’s Executive, Standards, and Operations Committees and have some material role in establishing and implementing PCI DSS. All of those attempts have been rejected by the networks. Today, retailers that accept credit or debit cards are kept completely out of all critical PCI decision-making processes and do not have the ability to assess and voluntarily adopt these requirements, let alone determine whether their business will be governed by PCI’s mandated security scheme.

In sum, the founding networks are the sole members of all PCI committees and control all technical and operational functions of the organization, including: setting PCI policies and priorities, establishing PCI DSS, implementing PCI DSS, and enforcing PCI DSS. Other (i.e., non-network) members of PCI have very limited opportunities to offer *non-binding* recommendations and feedback to the founding networks on PCI DSS issues. But again, retailers and other non-founding members have no control or authority with respect to standard-setting or PCI DSS compliance requirements, nor the ability to determine whether they will be governed by these mandates

D. Scope of PCI Standards and Network Control

PCI’s central function is to establish data security standards, which are enforced through the networks’ respective operating rule requirements.⁸ PCI DSS establish the operational and technical requirements for “all system components included in or connected to the cardholder data environment” and apply to all entities involved in payment card processing, including: merchants, processors, acquiring and issuing banks, and service providers (e.g., software developers and hardware manufacturers supplying equipment for use in transactions).⁹

⁸ See, e.g., Visa Supplemental Requirements List, Appendix A to Visa Core Rules and Visa Product and Service Rules (Oct. 16, 2015), *available at* <https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf> (last visited Mar. 22, 2016).

⁹ Payment Card Industry Data Security Standard, Requirements and Security Assessment Procedures, version 3.1, at 7, 10 (April 2015), *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf (hereinafter “PCI DSS Requirements”).

PCI DSS requirements cover the following broad areas for all entities in the payment system that process, store or transmit cardholder data and/or sensitive authentication data (e.g., merchants, network service providers, and acquiring banks):

- Building and maintaining a secure network and systems;
- Protecting cardholder data;
- Maintaining a vulnerability management program;
- Implementing strong access control measures;
- Regularly monitoring and testing networks; and
- Maintaining an information security policy.¹⁰

In total, across these areas, PCI imposes hundreds of discrete security requirements on merchants and other industry participants.¹¹

PCI claims to establish requirements for annual PCI DSS compliance assessments of all entities involved in the flow of cardholder data, including third-party service providers hired by merchants to help handle their data security functions. PCI qualifies entities as “Qualified Security Assessors,” thereby controlling the selection and supply of accredited PCI DSS compliance auditors. PCI also establishes the testing procedures that must be used for assessors to validate compliance with each specific PCI DSS requirement.

Assessed entities are further required by PCI to file Reports on Compliance with *each* network with which they do business (i.e., accept and process their brand of card).¹² Each network has its own reporting requirements, and each network must acknowledge an entity’s PCI DSS assessment compliance status.

A notable subset of PCI DSS requirements are payment application data security standards (“PA DSS”).¹³ PA DSS—which again include PCI-certified assessors, regular assessments, and specified testing procedures—apply to software vendors who develop payment applications that store, process, or transmit cardholder data or sensitive authentication data. Vendors may seek PA DSS validation for their software separately or as applications on hardware terminals.

¹⁰ PCI DSS Quick Reference Guide, v. 3.1 (May 2015), at 9, *available at* https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf.

¹¹ *See generally* PCI DSS Requirements.

¹² *Id.* at 17.

¹³ *See generally* Payment Card Industry Payment Application Data Security Standard, Requirements and Security Assessment Procedures, version 3.1 (May 2015), *available at* https://www.pcisecuritystandards.org/documents/PA-DSS_v3-1.pdf (hereinafter “PA DSS Requirements”).

Consistent with its command and control structure, PCI maintains a list of approved hardware terminals (i.e., devices through which payment cards are accepted at points of sale), and establishes approval and testing requirements (including approved labs for conducting testing) for those devices as well.¹⁴

Through hundreds of pages of technical requirements spread across (and cross-referencing) numerous documents, PCI's founding networks maintain a veritable web of control over every aspect of transaction processing, from approved software and hardware, to network and computer system maintenance, to annual audits and approved auditors, to ongoing reporting requirements to the networks with respect to PCI DSS compliance. At every step of the way, PCI dictates merchants' choices with respect to eligible third-party service providers, software and hardware vendors, approved equipment, certified auditors, etc. The networks, in turn, reinforce PCI's control over these products and business relationships by incorporating PCI's approved/certified entities and products directly into their own operating rules.¹⁵

The ultimate result of PCI's structure and activities is a complex and costly system in which merchants bear the compliance burden (with the attendant costs and risk) but are not permitted to participate in any decision-making.

II. Problems with Any Government Reliance on PCI Standards

A. PCI Does Not Satisfy Globally Accepted Principles for Standards Development

PCI does not follow standard-setting principles recognized by the U.S. government. The United States Standards Strategy ("USSS"),¹⁶ a document endorsed by U.S. agencies and published by

¹⁴ See generally Payment Card Industry PIN Transaction Security, Device Testing and Approval Program Guide, version 1.5 (July 2015), available at https://www.pcisecuritystandards.org/documents/PTS_Program_Guide_v1-5_July_2015.pdf; Payment Card Industry PIN Transaction Security Point of Interaction, Modular Security Requirements, version 4.1c (Nov. 2015), available at https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_SRs_v4-1c-November.pdf.

¹⁵ See, e.g., Visa Approved Security Assessors List (Feb. 29, 2016), available at <https://usa.visa.com/dam/VCOM/download/security/documents/sa-global-list.pdf>; MasterCard Qualified Security Accessor List, available at http://www.mastercard.com/us/sdp/vendors/assessor_list.html (last visited Mar. 30, 2016); American Express List of Assessors, available at <https://www.americanexpress.com/in/content/merchant/support/data-security/PCI-security-standards.html> (last visited Mar. 30, 2016).

¹⁶ Available at <http://trade.gov/td/standards/United%20States/US%20Standards%20Strategy-%20English.pdf>.

the American National Standards Institute (“ANSI”),¹⁷ sets forth the U.S.’s commitment to internationally accepted principles of standardization. Importantly, as a member of the World Trade Organization’s Technical Barriers to Trade Agreement, the U.S. government is responsible for supporting standardization practices that are in *full compliance* with these principles.¹⁸

These accepted principles include:

- **Transparency** - Essential information regarding standardization activities is accessible to all interested parties;
- **Openness** - Participation is open to all affected interests;
- **Impartiality** - No one interest dominates the process or is favored over another;
- **Effectiveness and Relevance** - Standards are relevant and effectively respond to regulatory and market needs, as well as scientific and technological developments;
- **Consensus** - Decisions are reached through consensus among those affected;
- **Performance Based** - Standards are performance based (specifying essential characteristics rather than detailed designs) where possible;
- **Coherence** - The process encourages coherence to avoid overlapping and conflicting standards;
- **Due Process** - Standards development accords with due process so that all views are considered and appeals are possible; and
- **Technical Assistance** - Assistance is offered to developing countries in the formulation and application of standards.

PCI does not satisfy *any* of these principles.¹⁹ The founding networks maintain exclusive control over all PCI committees and work and, despite numerous requests by retail groups to be given more access and a meaningful role in PCI, refuse to allow merchant participation in standard-setting activities (aside from after-the-fact opportunities to provide non-binding feedback).

¹⁷ ANSI is a private, non-profit organization comprised of businesses, trade associations, government agencies, international bodies, and consumer and labor organizations, and is the leading U.S. organization for coordinating and promoting voluntary consensus standards. ANSI is also the official U.S. representative to the International Organization for Standardization and other regional bodies focused on standardization.

¹⁸ The WTO Technical Barriers to Trade (“TBT”) Agreement was entered into on January 1, 1995. It “aims to ensure that technical regulations, standards, testing and certification procedures do not create unnecessary obstacles to trade.” The WTO Agreements Series; Technical Barriers to Trade, *available at* https://www.wto.org/english/res_e/publications_e/tbttotrade_e.pdf.

¹⁹ We are not aware of any technical assistance provided by PCI to developing countries with respect to development and application of standards, but such activities go beyond the scope of this paper.

Thus, PCI's standardization operations can hardly be considered transparent, open to affected parties, impartial toward non-network entities within the payment card industry, or based on consensus among affected parties. PCI's closed, network-dominated processes are in fact the antithesis of these principles.

PCI also neglects to provide due process to non-network industry participants (e.g., merchants) who wish to challenge PCI's standards, especially since, in light of the card networks' market power, it is highly impracticable for a merchant to simply walk away from accepting credit cards once it has a history with its customers of accepting those forms of payment. PCI instead cuts merchants and other affected parties out of the initial decision-making process and provides no opportunity for those affected parties to appeal for changes. PCI employs a top-down, take-it-or-leave-it approach to standards setting (i.e., go along with PCI's standards, which are memorialized in the card networks' operating rules, or face penalties and/or not be able to accept payment cards).

Further, PCI's standards do not prioritize effectiveness or performance-based measures of success. Rather, PCI imposes detailed, highly complex, costly technical specifications on merchants covering *all* aspects of transaction processing, including eligible parties and products that may be involved in the system.

Despite the breadth of requirements imposed on card-accepting merchants, PCI DSS *do not* maximize security or fraud prevention in the payment card system. PCI *could* take a simple, readily-implementable and relatively inexpensive step to vastly improve transaction security. Specifically, PCI's founding networks could require entry of a Personal Identification Number ("PIN") for every card transaction. Indeed, the Federal Reserve Board has found that PIN authentication is *six times* more secure than non-PIN (i.e., signature or simply swiping) authentication.²⁰ And yet, the networks have not imposed such a requirement, and instead, mandate an entire complicated (and very costly) scheme that purports to set minimum security standards for the industry.

Utilizing a model similar to PCI,²¹ in October 2015, the networks imposed a policy that merchants must accept EMV (i.e., chip cards) and be certified by each network as EMV-compliant, or else be liable for all fraudulent credit and debit card transactions involving chip-embedded cards. The EMV mandate required merchants to spend thousands of dollars per store

²⁰ Federal Reserve Board, Debit Card Interchange Fees and Routing, 77 Fed. Reg. at 46,261 (Aug. 3, 2010), available at <http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf>.

²¹ In this instance, Visa and MasterCard gave the rights to EMV technology to EMVCo (an organization controlled exclusively by the payment card networks), and EMVCo set proprietary standards for implementing that technology.

on software and hardware upgrades and programming new equipment to EMVCo network specifications, as well as the time and expense to get certifications of all new equipment from each of the different networks. All EMV equipment (including software, hardware, and security measures) must also satisfy PCI DSS, PA DSS, and PCI's device standards.

Throughout the rest of the world, the networks have imposed a chip-and-PIN policy. For the U.S., however, the networks have adopted a *chip-only* policy. Again, given the relative simplicity, low expense, and effectiveness of requiring PIN, it defies logic and recognized standard-setting principles that the networks would choose instead to mandate a new EMV regime (with all of its attendant costs and complications) and not take the additional step to require PINs for chip cards to maximize security in the U.S. payment card system as it does in Europe, Asia, the U.K., Canada, and the largest global economies.

In light of the successful worldwide deployment of chip-and-PIN, one might question why an open standard-setting body genuinely concerned with protecting the payments system did not require the use of PINs to promote better security here in the U.S. But PCI is not an open organization founded to maximize results. It is a proprietary organization dominated by a single interest group—the networks—with motivations apart from, and in conflict with, the interests of other payment card system participants on whom PCI's requirements are being imposed. Its “standards” should not be relied upon by any government body, in part because the process by which they are developed is fatally flawed.

B. PCI is Not a Qualified Standards Development Organization or Voluntary Consensus Standards Body Recognized by the U.S. Government.

In 2004, Congress enacted the Standards Development Organization Advancement Act (“SDO Act”).²² The purpose of the SDO Act was to provide relief from liability under the federal antitrust laws for qualified SDOs. A “Standards Development Organization” is defined under the SDO Act as:

[A] domestic or international organization that plans, develops, establishes, or coordinates voluntary consensus standards using procedures that incorporate the attributes of openness, balance of interests, due process, an appeals process, and consensus in a manner consistent with the Office of Management and Budget Circular Number A-119, as revised February 10, 1998.²³

²² Pub. L. No. 108-237, 118 Stat. 661.

²³ 15 U.S.C. § 4301(a)(8).

OMB Circular A-119 “establishes policies on Federal use and development of voluntary consensus standards and on conformity assessment activities.”²⁴ The Circular was initially developed in response to the National Technology Transfer and Advancement Act of 1995 (“NTTA Act”), which directs the federal agencies to “use technical standards that are developed and adopted by voluntary consensus standard bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments.”²⁵

Under the OMB Circular, “voluntary consensus standards” are standards “developed or adopted by voluntary consensus bodies [and] include provisions requiring that owners of relevant intellectual property have agreed to make that intellectual property available on a non-discriminatory, royalty-free or reasonable royalty basis to all interested parties.”²⁶ A “voluntary consensus standards body,” in turn, is:

[D]efined by the following attributes:

- (i) Openness;
- (ii) Balance of interest;
- (iii) Due process;
- (iv) An appeals process;
- (v) Consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objections(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.²⁷

Thus, under federal law, qualified SDOs that are eligible to receive antitrust relief and qualified voluntary consensus standards that are approved for federal agency use in lieu of government-unique standards must have these attributes. Again, PCI lacks *all* of them.

²⁴ Office of Management and Budget, Circular No. A-119 Revised, Memorandum for Heads of Executive Departments and Agencies (Feb. 10, 1998), available at https://www.whitehouse.gov/omb/circulars_a119/ (hereinafter “OMB Circular A-119”).

²⁵ Pub. L. No. 104-113, 110 Stat. 783.

²⁶ OMB Circular A-119.

²⁷ *Id.*

As discussed in detail above, PCI is not open to affected parties other than the networks. PCI favors banks, on which the networks rely to issue their cards, at the expense of merchants. There is no balance of interests because network interests are the only ones represented on PCI's committees and in the resulting standards. To the extent PCI takes into account any other participants in the payment card industry, it favors the banks on whom the networks rely to issue cards.

Finally, PCI's standards are not based on consensus. PCI DSS are dictated to payment card industry participants—particularly retailers—by the major card networks. In fact, merchants' requests to be part of PCI's standard-setting activities and serve on the Standards Committee have been refused. Thus, merchant comments are not considered during the standard-setting process or in the development of any compliance requirements. Instead, merchant comments on, and objections to, PCI DSS and related network operating rules are routinely dismissed by PCI's leadership. There are also no due process or appeals opportunities in place within the PCI structure.

Congress and the federal agencies have laid out a clear policy and plainly defined the types of standard-setting bodies that are entitled to antitrust relief and deference to and use of their standards by the federal government. PCI simply does not qualify as such a body.

C. PCI Presents Significant Antitrust Concerns

PCI's processes, standards, and compliance requirements also raise antitrust concerns. In 2007, the FTC and the Department of Justice ("DOJ") issued a document entitled "Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition" ("FTC/DOJ Paper").²⁸ The paper recognizes that standards adopted through collaborative standard-setting organizations ("SSO") can produce substantial economic and consumer benefits, but they can also "reduce competition and consumer choice and have the potential to prescribe the direction in which a market will develop."²⁹ Accordingly, the document notes, courts are sensitive to antitrust issues arising out of SSO activities.³⁰

²⁸ U.S. Department of Justice and Federal Trade Commission, *Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition* (April 2007), available at <https://www.ftc.gov/sites/default/files/documents/reports/antitrust-enforcement-and-intellectual-property-rights-promoting-innovation-and-competition-report.s.department-justice-and-federal-trade-commission/p040101promotinginnovationandcompetitionrpt0704.pdf> (hereinafter "FTC/DOJ IP Paper").

²⁹ *Id.* at 33-34.

³⁰ *Id.* at 34.

Aside from general antitrust dangers when competitors collaborate on setting market standards (while excluding other companies or market participants from discussions), PCI's actions raise more targeted concerns insofar as they allow the networks to leverage their proprietary technology through PCI DSS. The FTC/DOJ Paper addresses situations in which SSO standards incorporate technologies that are protected by intellectual property ("IP") rights. In those cases, the chosen technologies become essential (i.e., lacking competition or substitutes) because the SSO has picked them as the standard.

These scenarios present issues of "hold up" by the owner of the technology after the technology has been adopted as part of a standard. Because of sunk costs, it becomes difficult or cost prohibitive for merchants to switch to a different standard or technology. Put another way, as with PCI, the technology owners occupy all of the available dollars or "spend" and starve the market for innovators and new technologies. Then, the technology owners can extract unfair royalties and licensing terms because of the lack of competition, and consumers may be harmed in the form of higher prices.³¹ In turn, security suffers because innovations that might otherwise have advanced security have no foothold in the market and never develop. In this respect, PCI acts as an anticompetitive barrier to innovation because the payments system participant market (e.g., retailers) exhaust available resources complying with PCI's ever-changing security requirements.

Some SSOs have policies to mitigate hold up problems, which include, among other things, requiring advance disclosure of proprietary technologies that might be used in a standard and *ex ante* negotiations over post-standard licensing and royalty terms for the technology in question. Per the FTC/DOJ Paper, neither agency supports or requires any particular disclosure or licensing policy. The agencies do recognize, however, "the strong potential for procompetitive benefits" associated with such remedial actions (as long as those actions are structured properly and do not themselves cause antitrust problems).³²

PCI raises antitrust concerns around hold up, and to our knowledge, does not require or even encourage any disclosure or negotiations by the networks regarding their proprietary technology used in, or advanced by, PCI DSS. As one example, the PCI founding networks, along with China UnionPay Company, control—in virtually the same way they control PCI—EMVCo. EMVCo manages the technical specifications and testing processes for EMV (named for the Europay, MasterCard and Visa card brands), which is the proprietary technology in chip-embedded payment cards. The EMV technology is owned by the EMVCo networks (i.e., the PCI networks plus China UnionPay).

³¹ *Id.* at 35-36.

³² *Id.* at 53-54.

As noted above, beginning October 1, 2015, PCI's controlling networks imposed a policy that merchants must accept EMV (i.e., chip cards) and be certified by each network as EMV-compliant, or else be liable for all fraudulent transactions involving chip-embedded cards. The EMV mandate was effectuated in the same way PCI operates—without any input from non-network affected parties (i.e., merchants, banks, processors, etc.) and through a top-down, take-it-or-leave-it compliance approach.

The EMV transition required merchants to spend thousands of dollars per store, in addition to the annual budgeted expenditures to maintain their PCI compliance, on software and hardware upgrades and programming new equipment to EMVCo network specifications, as well as the time and expense to get certifications of all new equipment from each of the different networks.³³ Of course, all EMV equipment (including software, hardware, and security measures) must also satisfy PCI DSS, PA DSS, and PCI's device standards discussed above.

PCI openly pressures merchants to adopt EMV card reader technology. In PCI's own words:

The PCI Security Standards Council plays a significant role in the EMV chip rollout in two ways. PCI Standards – particularly PIN Transaction Security – are vital for protecting cardholder data entered at the point-of-sale and onward through the payment system. PCI Standards also are an essential compliment to EMV chip technology for each addresses different aspects of payment security. Merchants should use PCI-approved point-of-sale devices that include EMV chip functionality.³⁴

PCI also disseminates materials pairing its standards with the EMV proprietary technology.³⁵ PCI has even produced at least one video to pressure merchants to switch to EMV card acceptance technology.³⁶

Aside from separate antitrust concerns presented by EMVCo, the interconnectedness and hold up opportunities between PCI, EMVCo, and EMV should cause the FTC Commissioners (along with the Bureau of Competition) significant worry. The networks set the terms of the transition to their own proprietary technology, which necessitated system-wide shifts in software, hardware, and security measures, which are in turn controlled, certified, and approved by PCI.

³³ These expenditures are in addition to the cost of PCI compliance.

³⁴ Available at https://www.pcisecuritystandards.org/pdfs/Merchant_Guide_-_Stepping_Up_to_EMV_Chip_with_PCI_-_v06.pdf.

³⁵ Available at <https://www.pcisecuritystandards.org/pdfs/PCI-EMV-Final1.pdf>.

³⁶ Available at <https://www.youtube.com/watch?v=PoQwUT31Lgg>.

Neither network-controlled body can operate without the support of, and full coordination with, the other. And all of the respective mandates and requirements are enforced through the networks' respective operating rules.

Notably, *none* of the standards or requirements set by PCI, EMVCo, or the network operating rules are the product of open, balanced, or consensus-driven processes. Merchants in particular are left out of all decision-making and negotiations in all of these contexts. There is no opportunity for merchants or other market participants to effectively challenge or appeal any standards. And there certainly is no opportunity for merchants to negotiate *ex ante* over cost or licensing terms of the networks' proprietary technology or approved software, devices, assessors, etc.

The networks, in other words, unfairly leverage their brands and proprietary technology through webs of closely controlled interdependent bodies and compliance regimes. PCI is very much a part of this overall anticompetitive scheme. The FTC should be very mindful of the anticompetitive nature of PCI and the effects of its standards and processes before placing the government's imprimatur on PCI-DSS as reasonable data security standards for card-accepting businesses.

D. PCI has Conflicts of Interest and Misaligned Incentives Vis-à-Vis Other Industry Participants and Consumers

In addition to the aforementioned legal and policy concerns, PCI's structure and processes present clear conflict of interest problems. Because PCI is controlled by a single interest group within the payment card industry, its natural tendency is to protect that group's interests to the detriment of other stakeholders. We see this borne out in practice.

First, PCI is a cost-shifting organization that places a disproportionate amount of the compliance burden on merchants. Banks are spared from the same treatment because the banks are the networks' customers (i.e., the networks want to be the brand on issuing banks' cards). PCI's hundreds of security standards boil down to requirements that merchants invest in particular software, hardware, security measures, annual upgrades, assessment preparations, etc. According to Gartner's Retail Security & Compliance Survey for 2011, merchants spend an average of \$1.7 million over 2.35 years on PCI compliance, and that excludes the cost of assessors.³⁷ Again, these costs are imposed without any merchant involvement in any step of the process.

³⁷ Reuters, Press Release: *StillSecure Releases New PCI Compliance Cost Calculator for Level 1-4 Retailers* (July 6, 2011), available at <http://www.reuters.com/article/idUS120097+06-Jul-2011+MW20110706>.

Second, because PCI's founding networks can shift costs associated with data security—and notably, data breaches³⁸—onto merchants and other stakeholders, and simultaneously benefit from the required use of their proprietary technology, PCI is not incentivized to adopt the most effective security measures. If it were interested in maximizing security, as noted above, PCI would—at a minimum—require financial institutions to invest in PINs to enable all parties to better secure card transactions.

PINs are simple, low-cost, and proven to reduce fraud losses in the payment card system. In fact, the networks themselves promote the security benefits of PIN. In 2013, for example, Visa and MasterCard jointly petitioned the Australian Competition and Consumer Commission for authorization to *require* PIN authentication on transactions involving their cards.³⁹ In their application, they made numerous statements in support of requiring PIN at the point of sale, including:

“The Applicants’ view is that chip and PIN is a significantly more secure form of [customer verification method] than signature.”

“Based on the experience of the introduction of mandatory PIN@POS [Point of Sale] in overseas markets (in the UK, Canada, Europe and elsewhere), the Applicants expect that certain types of card present fraud will decline in Australia as a result of the introduction of mandatory PIN@POS in Australia.”

“The Applicants note that overseas experience has shown that fraud will move to jurisdictions where there are lower security measures in place and in particular jurisdictions that do not use EMV and PIN security. For example, the UK experience has been that the countries where fraud on UK-issued cards occurs has changed with fraudsters focusing on countries without ‘chip and PIN,’ such as the United States. There has been a similar experience in Europe. Card fraud is highly mobile and is often internationally organized. The coordinated

³⁸ Aside from the liability shift associated with the EMV transition, merchants have historically paid the majority of fraud losses. Despite banks’ claims that they provide a “payment guarantee,” merchants are absorbing the vast majority of the costs associated with fraudulent transactions. *See* Press Release: *U.S. Retailers Face \$191 Billion in Fraud Losses Each Year*, LexisNexis Risk Solutions (Nov. 9, 2009) (highlighting findings of LexisNexis and Javelin Strategy & Research “True Cost of Fraud Benchmark Study”), *available at* <http://www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1258571377346174>. And, merchants’ fraud losses have kept going up with the revenue lost nearly doubling from 2014 to 2015. 2015 LexisNexis True Cost of Fraud Study, Sept. 2015 *available at* <http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx>. *See also* *House of Cards: Why your accounts are vulnerable to thieves* (June 2011).

³⁹ *See generally*, Visa & MasterCard – Authorisations – A91379 & A91380, *available at* <http://registers.accc.gov.au/content/index.phtml?itemId=1120516>.

introduction of mandatory PIN@POS in Australia will increase card security in Australia and make it a less attractive jurisdiction for fraudsters.”

“The Applicants believe that mandatory PIN@POS is an important step in the right direction, in terms of reducing credit card fraud in Australia.”⁴⁰

Despite these representations to the Australian authorities and the networks’ affirmative recognition that the use of PIN does improve transaction security, PCI has declined to advance the use of PIN here in the U.S. Instead, they have opted to support a chip-without-PIN regime through PCI DSS and the networks’ individual operating rules—a move that simply cannot be justified given their own experience and data.

Ultimately, consumers also suffer under the PCI system. First, it does not minimize payment card fraud. Second, the substantial cost of PCI compliance is at least partially passed through in the form of higher prices. And finally, because consumers are also excluded from PCI processes, their views are ignored and they have no opportunity to help develop a competitive, efficient, consensus-based data security solution.

If it relies on PCI DSS as a baseline for FTC data security actions, the FTC risks entrenching proprietary standards that are the result of illegitimate processes, do not adequately protect security, and raise competition policy concerns. PCI is not representative of the entire industry, and in fact, the networks are flatly at odds with other stakeholders. The FTC should not sanction (or even appear to sanction) PCI’s cost-shifting model or its inefficient approach to data security.

III. Recommended Actions

As more fully discussed above, there is a need to address the problems that PCI has created by promulgating proprietary specifications that are not actually standards, and having its controlling networks foist them on the payment card system as though they were standards. We recommend the FTC consider the following actions in determining how best to address these significant concerns surrounding PCI and PCI DSS:

- Investigate PCI’s Processes. The FTC should investigate the PCI standard-setting process to reach its own conclusions regarding the processes employed by PCI and whether those processes meet the requirements for standard-setting laid out by federal law and policy.

⁴⁰ Submission of Visa Worldwide, Visa AP (Australia), and MasterCard Asia/Pacific to the Australian Competition & Consumer Commission in support of Authorisations A91379 & A91380 (Aug. 30, 2013), “Security of Chip and PIN vs. Signature,” pp. 1-2, *available at* <http://registers.accc.gov.au/content/index.phtml?itemId=1120516&display=submission> (last visited Sept. 21, 2015).

- Investigate PCI's Competition Impacts. The FTC should investigate the PCI standards and how those standards are implemented and enforced by the payment card networks that run PCI in order to determine whether the standards and their implementation violate competition laws.
- Reject the Use of PCI Standards as a Benchmark for Data Security. Given the facial problems with PCI's processes and standards, the FTC should not in any way rely on those standards as indicia of an industry-wide standard with respect to data security or any other matter.
- Work with Legitimate Standard-Setting Bodies. Rather than relying upon the flawed PCI standards, the FTC should work with legitimate U.S. standard-setting bodies such as ANSI to ensure that standards for the payment card industry and card security are set in a manner that is consistent with the U.S. Standards Strategy and competition policy.

By taking these actions, the FTC can head off the problems PCI is creating throughout the payments system and establish the groundwork for standard-setting that advances U.S. policy interests in data security.