ROPES & GRAY

ALERT

Privacy & Data Security

March 31, 2016

FTC Launches Study of Assessment Process for Payment Card Industry Data Security Standards

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David M. McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
David T. Cohen

On March 7, the FTC announced a study of Payment Card Industry Data Security Standard ("PCI DSS") assessments – the audits required of certain merchants pursuant to rules imposed by payment card brands such as Visa and MasterCard. As part of this study, the FTC issued orders to provide information to nine data security auditors.[1] While the FTC announcement does not specify a motivation for the study or how its results might be used, the level of detail of the FTC's questions and the depth of required responses suggests that the FTC's interest in the PCI DSS is more than a passing one. Companies required to maintain PCI DSS certification should be aware of the possibility that FTC involvement could lead to changes in the PCI DSS certification process, including a more stringent, and costly, assessment process.

On March 7, the FTC announced a study of Payment Card Industry Data Security Standard ("PCI DSS") assessments – the audits required of certain merchants pursuant to rules imposed by payment card brands such as Visa and MasterCard. As part of this study, the FTC issued orders to provide information to nine data security auditors.[2] While the FTC announcement does not specify a motivation for the study or how its results might be used, the level of detail of the FTC's questions and the depth of required responses suggests that the FTC's interest in the PCI DSS is more than a passing one. Companies required to maintain PCI DSS certification should be aware of the possibility that FTC involvement could lead to changes in the PCI DSS certification process, including a more stringent, and costly, assessment process.

Many of the FTC's requests for information are geared generally toward the degree of rigor in, and the efficacy of, PCI DSS assessments. For example, the FTC asks about certifications and training required of the PCI DSS assessors, the time spent on a typical PCI DSS assessment, the number of assessments that found PCI DSS compliance, the number of assessments that designated clients as non-compliant, and the number of clients who suffered a data breach in the year following an assessment. Several of the FTC's questions, however, are at a level of detail that suggests the FTC has given a great deal of thought to what the agency may perceive as potential weaknesses in the PCI DSS certification process. In particular, the FTC directs questions toward assessment scope,[3] sampling

[1] The nine companies are Foresite MSP, LLC, Freed Maxick CPAs, P.C.; GuidePoint Security, LLC; Mandiant; NDB LLP; PricewaterhouseCoopers LLP; SecurityMetrics; Sword and Shield Enterprise Security, Inc.; and Verizon Enterprise Solutions (aka CyberTrust). Companies that have hired any of the nine particular data security assessors that are the present subjects of the study might consider asking these assessors whether documents related to their own PCI DSS assessments have been or will be produced to the FTC.

[2] The nine companies are Foresite MSP, LLC, Freed Maxick CPAs, P.C.; GuidePoint Security, LLC; Mandiant; NDB LLP; PricewaterhouseCoopers LLP; SecurityMetrics; Sword and Shield Enterprise Security, Inc.; and Verizon Enterprise Solutions (aka CyberTrust). Companies that have hired any of the nine particular data security assessors that are the present subjects of the study might consider asking these assessors whether documents related to their own PCI DSS assessments have been or will be produced to the FTC.

[3] An initial determination of the proper scope of a PCI DSS assessment can preclude assessment of systems that are deemed sufficiently segregated from the Cardholder Data Environment and can have a significant effect on the overall cost of a PCI DSS assessment. *See* PCI DSS v.3.1, at 10-11.

procedures, reliance on employee interviews, and compensating controls.[4] The theme of potential conflicts of interest also comes up repeatedly. The FTC asks directly about policies regarding conflicts of interest both for standard PCI DSS assessments and for forensic audits performed after a data breach, and asks several more specific questions related to the independence of assessors. For example, the FTC asks whether clients have input into the drafting of assessment reports, the extent to which a client has input into the scope of a PCI DSS assessment, and the extent to which the assessor communicates with the client in determining the adequacy of compensating controls.

The FTC requests not just narrative responses from the nine data security companies, but also documents related to six representative assessments,[5] including contracts, notes, test results, and communications with the client or third parties.

The FTC did not explain the study's purpose other than to say that information gathered will be "used to study the state of PCI DSS assessments," but the study may simply be a means of settling an ongoing disagreement within the FTC as to how reliable certified PCI DSS compliance is as an indicator of reasonable data security. The FTC has previously relied upon PCI DSS compliance as an indicator of reasonable data security. Under the terms of the FTC's settlement with hospitality company Wyndham Hotels and Resorts, the requirement that Wyndham maintain reasonable information security was deemed to be satisfied if Wyndham maintained certification of PCI DSS compliance.[6] Last year, however, the FTC sued LifeLock, Inc. and reached a $100,000,000 settlement, on allegations that LifeLock violated a 2010 data security consent order by, among other things, failing to maintain adequate data security despite the fact that LifeLock maintained PCI DSS certification.[7] In a vigorous dissent to the proposed settlement, Commissioner Ohlhausen specifically pointed to the Wyndham settlement to show that "the FTC considers PCI DSS certifications to be important evidence of reasonable data security." In response, Chairwoman Ramirez, Commissioner Brill, and Commissioner McSweeny issued a public statement proclaiming that "[c]ertifications alone will not suffice" to meet obligations to protect consumer information through reasonable data security.

Given the FTC's aggressive stance toward data security enforcement generally, it seems quite possible that the FTC is not merely settling an internal debate over the merits of PCI DSS, but also seeks to influence the PCI DSS assessment process. To the extent that the FTC concludes that PCI DSS certification does not reliably indicate reasonable data security, the FTC could pressure the industry to apply more rigor to the PCI DSS assessment process. Pressure could be exerted upon the promulgators of the PCI DSS to revise formal requirements or upon merchants and other industry participants by according weight only to PCI DSS assessments that meet the FTC's own standards of adequacy. It is also possible that the FTC contemplates actions against data security companies performing the assessments on the theory that inadequate PCI DSS assessments can cause consumer harm through subsequent breaches.[8]

---

[4] "Compensating controls" are security measures that an assessor can deem sufficient to compensate for the lack of literal adherence to PCI DSS requirements "when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints." *See* PCI DSS v.3.1, at App. B.

[5] The FTC asks for documents related to two representative assessments completed last year, as well as documents related to representative assessments in which 1) sampling was used, 2) compensating controls were used, 3) draft reports were shared with clients, and 4) the client was allowed to remediate before certification was issued.

[6] In addition to certification of the extent of compliance with the PCI DSS or another approved standard, the settlement requires limited additional certifications, but these are all already encompassed by an assessment of full PCI DSS compliance: 1) whether Wyndham treats external franchisee networks as "untrusted" networks, 2) the extent of Wyndham's compliance with a risk protocol, and 3) that the PCI DSS assessor was qualified and independent.

[7] *FTC v. LifeLock, Inc.*, No. CV-10-00530-PHX-JJT (D. Ariz.).

[8] One could speculate from the FTC's question regarding the number of clients that were victims of data breaches that occurred within a year after an assessment that the FTC is interested in possible causal links between inadequate assessments and actual data security breaches. Such a focus on service providers would break new ground for FTC information security enforcement, though. The FTC has never previously entered into a consent order based on allegations that a service provider failed to provide adequate data security to protect personal information received by its client. (In litigation against Wyndham, the FTC alleged

While it is certainly possible that the FTC study portends future FTC pressure on the process of PCI DSS certification, such regulatory focus would make little sense for a regulator charged with protecting consumer interest. To begin with, even in an instance where an alleged failure to comply with the PCI DSS purportedly allowed a data compromise to occur, which in turn resulted in payment card fraud, the likelihood of actual consumer harm is remote because consumers are, as a rule, fully reimbursed for any fraud.[9] Moreover, PCI DSS certification is now of decreasing relevance as merchants are shifting to chip technology. Chip technology – which utilizes microchip-embedded cards – may drastically reduce counterfeit fraud associated with data breaches, and the major card brands now have programs to eliminate requirements of PCI DSS certification for qualified merchants that have implemented chip technology.[10] Indeed, given the promise of chip technology, it could be argued that any increased regulatory attention should be directed at card brands, which for years delayed implementing chip technology. (And when the card brands finally did implement chip technology – in a manner imposing onerous costs upon merchants[11] – it was a Chip and Signature version, which offers less security than the Chip and Pin version that has long been used throughout much of the world.[12]) Given this, it is possible that the purpose of the FTC study is not to place pressure on the PCI DSS certification process, but rather to simply understand it better so that the FTC can apply the lessons learned to advocate for similar models being adopted outside the payment card industry. That said, companies that undergo PCI DSS certifications should be aware that the FTC's interest in the PCI DSS certification process could forebode increased costs of certification in the event that FTC pressure results in a more stringent certification process.

For more information regarding the FTC's study of PCI DSS assessments, or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.

---

that Wyndham as a service provider to its franchisee hotels failed to provide adequate data security to protect the personal information collected by the franchisee hotels, but the FTC's final consent decree with Wyndham effectively dropped this theory, requiring only the protection of Wyndham's own data.)

[9] *See, e.g., Whalen v. Michaels Stores, Inc*., 14-CV-7006 (JS)(ARL), 2015 WL 9462108, at *3 (E.D.N.Y Dec. 28, 2015) (finding in wake of data security breach that there was insufficient injury to consumers to support Article III standing, where no unreimbursed payment card charges were alleged), *appeal docketed*, No. 0:16-cv-00260 (2d Cir. Jan. 27, 2016); *Burton v. MAPCO Express, Inc.*, 47 F. Supp. 3d 1279, 1284-85 (N.D. Ala. 2014) (same); *Hammond v. Bank of New York Mellon Corp*., No. 08 Civ. 6060 (RMB) (RLE), 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (same).

[10] *See* Visa, *Tap into the Power of EMV Chip Technology and Start Building Your Future Today*, at 2 (2015); MasterCard, *Security Rules and Procedures: Merchant Edition*, § 10.3.4.2 (Feb. 5, 2015); American Express, *Frequently Asked Questions: EMV Global and US*, at 5 (2013); Discover, *Momentum*, at 3 (2013).

[11] The burden upon merchants is great enough to inspire a putative class action in which merchants allege that an agreement among card brands to shift liability for counterfeit fraud to merchants as part of the shift to chip technology amounted to a conspiracy in violation of the Sherman Act. *B & R Supermarket, Inc. v. Visa*, Inc., No. 4:16-cv-001150 (N.D. Cal. Filed Mar. 8, 2016).

[12] As an example of recent regulatory interest in the card brands' inaction, in November 2015, eight state attorneys general sent a letter to major card brands and banks noting that the delay in adopting Chip and Pin technology could be considered unreasonable. See *Ropes & Gray Alert: State Attorneys General Fire Shot Across the Bow at Major Payment Card Brands Over "Chip and Pin" Technology* (Dec. 4, 2015).