PCI DSS and card brands: Standards, compliance and enforcement

Received (in revised form): 20th April, 2018

Donna Wilson

is a partner at Manatt, Phelps & Phillips, LLP and is nationally recognised for her high-profile, bet-the-company work on behalf of companies facing litigation and government enforcement actions, with a focus on both the consumer financial services and privacy and data security spaces. She is the chair of Manatt's privacy and data security practice and co-chair of its financial services group and financial services litigation and enforcement practice, and is also recognised by professional publications for leadership. Most recently, she was selected as one of twenty Top Cyber/Artificial Intelligence Lawyers and one of 100 Top Women Lawyers in California by the *Daily Journal*, and one of the Most Influential Women Lawyers in Los Angeles by the *Los Angeles Business Journal*. She is a frequent author, speaks on cutting-edge legal matters and is regularly quoted by various media, including the *Wall Street Journal*, *USA Today* and the *Daily Journal*.

Manatt, Phelps & Phillips, LLP, 11355 W. Olympic Blvd, Los Angeles, CA 90064, USA
Tel: +1 310 312-4144; E-mail: DLWilson@manatt.com

Ethan Roman

is a litigation and cyber security attorney in the New York office of Manatt, Phelps & Phillips, LLP, where he advises companies on a broad spectrum of issues, including data breach responses, security incident investigation, containment and mitigation and best practices and policies. He is a Certified Information Privacy Professional for the US Private Sector (CIPP/US) and an active member of the International Association of Privacy Professionals, where he serves as a Young Privacy Professional Leader for New York City.

Manatt, Phelps & Phillips, LLP, 7 Times Square, New York, NY 10036, USA
Tel: +1 212 790-4535; E-mail: EDRoman@manatt.com

Ingrid Beierly

is a Senior Advisor, Cyber and Global Payment Security at Manatt, Phelps & Phillips, LLP. A senior security risk business leader with a record of achievement in payment data security, she has led successful efforts to mitigate global payment risk and cyber security data compromises for impacted entities. Ingrid previously served as a global forensic and cyber intelligence business leader with a major credit card company for over a decade. As both analyst and advisor, she spearheaded global computer forensic investigations impacting credit card members, merchants and service providers, providing insight on fraud investigations, data security compromises and compliance preparation. Ingrid was instrumental in developing data security programmes, such as the Cardholder Information Security Program (now known as Payment Card Industry Data Security Standards), Payment Application Data Security Standards, Payment Forensic Investigator and Qualified Integrator and Reseller Program. These programmes impact entities all over the world. Before joining Manatt, Ingrid served as an independent payment security consultant in the San Francisco Bay area, focusing on payment data security, incident response and credit/debit/prepaid card fraud mitigation strategies for a high-profile clientele.

Manatt, Phelps & Phillips, LLP, One Embarcadero Center, 30th Floor, San Francisco, CA 94111, USA
Tel: +1 415 291-7408; E-mail: IBeierly@manatt.com

Abstract The payment card brands have a private regulatory system, the PCI DSS, that affects every entity worldwide that accepts, processes, stores or transmits credit card information. Participation is mandatory for companies to function in the modern economy, and the consequences of non-compliance can be harsh. A further complication is that the PCI DSS uses its own terminology, which can be confusing to a beginner. But there

are also benefits to understanding PCI compliance, including to avoid the potentially harsh consequences, and the fact that PCI compliant entities have a stronger defensive posture against cyberattacks. Because of this, all organisations should know about and understand the PCI DSS, including how to implement and maintain compliance. This paper outlines the history and reason behind the PCI DSS and the broad requirements entities must follow to be compliant; provides an overview of the basic terminology and requirements, information on additional programmes that affect an entity's PCI DSS compliance, a high-level view of compliance and information on its enforcement by the card brands, state legislation and the legal system; and offers some views from both critics and supporters of the current enforcement system.

KEYWORDS: PCI, PCI compliance, payment cards, PCI enforcement, cyber security

INTRODUCTION

The payment card industry and the major card brands have a set of data security requirements — PCI DSS — that are unregulated by government, yet every company worldwide that accepts, processes, stores or transmits credit card information must comply with and follow the card brands' rules. Failure to do so can result in penalties imposed by the card brands, or, for businesses, the inability to accept credit cards. Because of the potential consequences, understanding and complying with the PCI DSS is critical. This paper will introduce the history of the PCI DSS, define its commonly used terms, introduce the high-level requirements entities must follow to be compliant and certify their compliance, and review the litigation landscape as it relates to PCI.

HISTORY OF PCI DSS

The PCI DSS is a set of standards intended to encourage and enhance security for all entities that accept, process, store or transmit credit card information.[1] The Payment Card Industry Security Standards Council (PCI SSC or Council) was formed on 7th September, 2006. The major payment card brands — American Express, Discover Financial Services, JCB International, Mastercard Worldwide and Visa Inc. — founded the Council and remain its members in present day.

The PCI DSS is available on the Council's website.[2] It applies to all entities that accept, process, store or transmit cardholder data, including entities located outside the US,[3] meaning that every entity worldwide that accepts payment cards must comply with the PCI DSS. Entities include merchants, acquirers, issuers, service providers, processors and third-party agents. Although implementing PCI DSS is required for all entities that store, process or transmit cardholder data, formal validation of compliance is not mandated for all entities. Over the years, the PCI DSS has undergone several revisions, and is currently on version 3.2.

THE BASICS

PCI DSS has its own terminology and can be quite confusing to a newcomer. Here are definitions of some of the commonly used terms in PCI DSS, provided on the Council's website:

- **Acquirer**: Also referred to as 'merchant bank', 'acquiring bank' or 'acquiring financial institution'. Entity, typically a financial institution, that processes payment card transactions for entities and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding

merchant compliance. They must also ensure that their sponsored agents, processors and/or service providers that store, process or transmit card data comply with the PCI DSS.

- **Issuer**: Entity that issues payment cards or performs, facilitates or supports issuing services, including but not limited to issuing banks and issuing processors. Also referred to as 'issuing bank' or 'issuing financial institution'. Issuers are subject to payment brand rules and procedures and must ensure not only that they, but also that their sponsored agents, processors and/or service providers that store, process or transmit card data, comply with the PCI DSS.
- **Cardholder**: Non-consumer or consumer customer to whom a payment card is issued, or any individual authorised to use the payment card.
- **Cardholder data**: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.
- **Payment processor**: Sometimes referred to as 'payment gateway' or 'payment service provider' (PSP). Entity engaged by a merchant, acquirer, issuer or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
- **Third-party agents/service providers**: Organisations that store, process, transmit or have access to cardholder account or transaction information on behalf of acquirers, issuers, merchants, other service providers or payment processors.[4]

The Standards

The PCI DSS has 12 high-level requirements, which fall under six goals:

- Build and maintain a secure network
  1. Install and maintain a firewall configuration to protect cardholder data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters;
- Protect cardholder data
  3. Protect stored data
  4. Encrypt transmission of cardholder data across open, public networks;
- Maintain a vulnerability management programme
  5. Use and regularly update anti-virus software or programs
  6. Develop and maintain secure systems and applications;
- Implement strong access control measures
  7. Restrict access to cardholder data by business need-to-know
  8. Assign a unique ID to each person with computer access
  9. Restrict physical access to cardholder data;
- Regularly monitor and test networks
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes;
- Maintain an information security policy
  12. Maintain a policy that address information security for all personnel.

Included under these high-level standards are over 200 line item requirements.

For entities just setting out on the road to PCI DSS compliance, the Council provides a Prioritized Approach[5] to help entities incrementally protect against the highest risks and threats. The Prioritized Approach has six milestones:

1. Remove sensitive authentication data and limit data retention;
2. Protect systems and networks, and be prepared to respond to a system breach;
3. Secure payment card applications;
4. Monitor and control access to your systems;

5. Protect stored cardholder data;
6. Finalise remaining compliance efforts, and ensure all controls are in place.

ADDITIONAL PROGRAMMES THAT AFFECT AN ENTITY'S PCI DSS COMPLIANCE

Payment Application Data Security Standards (PA-DSS)[6]

PA-DSS defines security requirements for software vendors of payment applications. Entities that use a third-party payment application that stores, processes or transmits cardholder data or has access to cardholder data must ensure the application is PA-DSS compliant. The goal of PA-DSS is to ensure that the application does not hinder an entity's PCI DSS compliance and, when implemented in a secure manner, will minimise the potential for a data breach. PA-DSS is managed by the PCI SSC and the certification assessment is performed by a Payment Application Qualified Security Assessor (PA-QSA). The payment card brands require that entities utilise a PA-DSS compliant payment application. At a high level, the PA-DSS certification process involves the following steps:

1. Software vendor engages a PA-QSA to certify the application against PA-DSS;
2. Proof of certification via a Report of Validation (ROV) will be provided to the PCI SSC for review and acceptance;
3. Once the ROV is accepted by the PCI SSC, the payment application will be listed on the PCI SSC's website as compliant.

Compliant payment applications must be capable of being implemented in a PCI DSS compliant-manner. As part of the PA-DSS certification process, software vendors are required to provide an implementation guideline to their clients and other third-party entities that may manage or install the payment application.

Revalidation of the payment application by a PA-QSA is required if major changes are made to the application that affects a majority of the PA-DSS requirements.

Qualified Integrator Reseller (QIR) programme

QIRs are third-party companies engaged by an entity or software vendor to install and manage a payment application remotely. The QIR programme was initiated by Visa Inc. due to the increase of Level 4 merchant data compromises involving insecure remote access protocols and weak passwords utilised by third-party companies. The vulnerabilities allowed hackers to gain unauthorised access to Point-of-Sale (POS) systems and install malicious software to steal full magnetic stripe data. Furthermore, the same user ID and password is used for the third-party company's client-based system which allowed a wide-spread attack on numerous Level 4 merchants. In the last six months of 2016, insecure remote access through third-parties was the single largest origin of data compromises.[7]

In August 2012, the programme was handed over to the PCI SSC to manage the certification of QIRs. For a third-party company to become a certified QIR and be listed on PCI SSC's website, they must comply with the following:

1. Be a recognised legal company;
2. Adhere to PCI SSC's Code of Professional Responsibility;
3. Pay and take the PCI SSC's training exam;
4. Provide proof that the company is a direct provider of a PA-DSS validated payment application;
5. Each employee performing installations must have the skills and experience as listed on the QIR qualification requirements.

Using a certified QIR is not a requirement with the payment card brands, with the exception of Visa. On 29th October, 2015,

Visa announced a new mandate for US and Canadian acquirers. Effective from 31st March, 2016, acquirers must communicate to their Level 4 merchants that beginning on 31st January, 2017, merchants *must* use a certified QIR for POS installation and management.[8] In addition, Level 4 merchants must validate PCI DSS compliance or enrol in Visa's Technology Innovation Program (TIP).[9] TIP is an incentive programme for merchants to migrate to EMV[10] or Point-to-Point Encryption (P2PE). If a merchant enrols in TIP, the merchant will not be required to do an annual PCI DSS compliance validation, but they must still comply with PCI DSS. Visa mandated this new requirement to help reduce data compromises involving Level 4 merchants.

COMPLIANCE

As mentioned above, all entities that accept, process, store or transmit credit card information must comply with the PCI DSS. This is true even for entities that use third party payment processors.

But not every entity is held to the same standard, with the exception of Visa, as mentioned above. This makes sense — there is no need for an entity that processes a few hundred or 1,000 transactions annually to undergo the same level of rigour to satisfy the PCI DSS requirements as an entity that processes millions of transactions. This primarily comes into play when entities must validate their compliance with the PCI DSS. Regardless of transaction volume, all entities must pass a quarterly vulnerability scan, which must be performed by an Approved Scanning Vendor (ASV). But for additional validation requirements, entities are separated into four levels. Each payment card has its own standards, but, for example, Visa separates the merchant and service provider levels as follows:

Merchants:

- Level 1: Merchants that process over 6m transactions per year, or merchants who suffered a breach where data was compromised in the past year;
- Level 2: Between 1m and 6m transactions per year;
- Level 3: Between 20,000 and 2m e-commerce transactions per year;
- Level 4: Less than 20,000 e-commerce transactions, or less than 1m other types of transactions per year.[11]

Level 1 Visa merchants, in addition to the quarterly network scan, must annually file a Report on Compliance (ROC) by a Qualified Security Assessor (QSA) or, if the ROC is signed by an officer, by the merchant's internal auditor. QSAs are companies with trained personnel and processes to help entities assess compliance with the PCI DSS.

Level 2, 3 and 4 Visa merchants must complete a Self-Assessment Questionnaire (SAQ) and submit an Attestation of Compliance (AOC) form. It is important to keep in mind that each card brand has its own compliance programme. Mastercard, for instance, gives Level 2 merchants the option of bringing in a QSA for an onsite assessment, or conducting a SAQ.

Service Providers:

- Level 1: Processors or any service providers that store, process or transmit over 300,000 Visa transactions annually. Processors/service providers in this category must validate compliance annually by a QSA and perform a quarterly network scan by an approved ASV;
- Level 2: Any service providers that store, process or transmit less than 300,000 Visa transactions annually. Service providers in this category must complete a SAQ D annually and perform a quarterly network scan by an approved ASV.

As mentioned above, both Visa and Mastercard require service providers to be registered with their registration programmes

and must provide the AOC in order to be added to their Service Provider Compliant List.

Entities that store, process or transmit cardholder data is responsible for maintaining compliance with PCI DSS and that includes any outsourcing of payment card data. Outsourcing of payment card data include, but not limited to:

- Processing;
- Management;
- Accessing;
- Data warehousing.

The entity outsourcing the processing and/or managing of their data should perform their due diligence to ensure that their third-party service provider protects the data. As mentioned above, each payment card brands maintain a list of compliant service providers. Entities and acquirers should review the individual payment card brand site to ensure their service provider is PCI DSS compliant. If there is a breach involving payment card data (regardless of whether or not the data was outsourced) and the forensic investigation reveals that the compromised entity was in violation of PCI DSS, the payment card brands will levy a fine to the acquiring bank. We highly recommend entities review their service provider service level agreement and/or contracts and ensure, at a minimum, the following are addressed:

1. A clear understanding of roles and responsibilities as related to data security;
2. Requirement that their service provider undergo PCI DSS compliance;
3. Timely notification in the event of a suspected or confirmed data breach at the service provider environment. The notification should include you as the owner of the data, acquiring bank and payment card brands. The payment card brands have a requirement that they be notified of a suspected or confirmed breach within a certain time frame.[12] Delay in notification can result in significant penalties.
4. A robust incident response plan and testing the plan annually to ensure validity;
5. The ability to limit data exposure and minimise loss by having a robust incident response plan and following industry practice in preserving evidence.

Complying with the PCI DSS can seem like a burden, but there are also benefits. By following the PCI DSS, entities can improve their security posture for all data they collect and store, not just cardholder data. The steps required to comply with the PCI DSS can also help entities prevent and detect attacks against their systems, avoiding data breaches and the accompanying fines, investigations and/or litigation.

For entities that are required to comply with other regulations that may compete with the PCI DSS requirements, we recommend that they assess their business to identify the type of data they process, store, accept and transmit (eg credit card data, healthcare, personally identifiable information). Entities should work with their internal or external audit, legal/privacy, information security and third-party subject matter experts to map out and compare the requirements and develop a streamlined approach to compliance. Limiting data retention, as mentioned on the PCI prioritised approach, is a good start.

ENFORCEMENT

Compliance enforcement for the PCI DSS and determination and assessment of any penalties are carried out by the individual payment card brands.[13] There is no federal law requiring compliance with the PCI DSS. Most US state laws do not require compliance, but:

- Minnesota's Plastic Card Security Act requires any company that suffers a

data breach and is found to have been storing prohibited card data on its systems to reimburse financial institutions for the costs associated with blocking and reissuing cards;[14]
- Nevada and Washington mandate compliance with the PCI DSS, and compliance shields merchants from liability for damages resulting from a data breach.[15]

The card brands enforce compliance primarily through fines of the acquiring bank, which is the bank that processes card transactions for the merchant. The acquiring bank may be fined up to $100,000 per month for non-compliance, which it will likely pass on to the merchant or service provider.[16]

The PCI enforcement structure is not without its critics. At a hearing before the Congressional House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology on 31st March, 2009, people affiliated with the retail industry voiced their opinions on problems with PCI enforcement. Michael Jones, then-Chief Information Officer of Michaels Stores, testified that the PCI DSS requirements were 'developed from the perspective of the card companies rather than from those who are expected to follow them' and called the requirements 'very expensive to implement, confusing to comply with, and ultimately subjective both in their interpretation and in their enforcement'.[17] At the same hearing, David Hogan, then-Senior Vice President, Retail Operations and Chief Information Officer for the National Retail Federation, accused the card brands of using the PCI framework as 'a tool to shift risk off the banks and credit cards' balance sheets and place it on others', noting that under the PCI DSS, entities were required to store unwanted credit card data for long periods of time.[18]

Other criticisms of PCI DSS enforcement focus on the payment card brands' actions surrounding data breaches for PCI compliant companies. For example, in 2009, payment processing companies Heartland Payment Systems Inc. and RBS WorldPay Inc. were removed from Visa's list of compliant companies after they suffered data breaches.[19] Critics of Visa's action cast it as an attempt to insulate Visa from any ensuing litigation because of Visa's rule that compliant companies who suffer breaches can avoid fines.[20] An analyst at one technology research company called Visa's decision 'legal maneuvering', accusing Visa of conducting 'PCI enforcement as usual' by 'making the rules up as they go'.[21]

Lawsuits between merchants and payment card brands have had mixed results for merchants. In *Genesco v. Visa, Inc.*, Visa had imposed approximately $13.3m in non-compliance fines. Genesco sued for recovery of the fines, alleging that it was 'at all relevant times … in compliance with the PCI DSS requirements'.[22] The court denied Visa's motion to dismiss claims under California's unjust competition law and unjust enrichment, and Genesco's motion for summary judgment, but the case settled before trial.[23] But that was a good result for the merchant when compared to *Jetro Holdings, LLC v. MasterCard Int'l, Inc.*, where a New York state court granted Mastercard's motion to dismiss.[24] Following two breaches of Jetro's network, Mastercard imposed approximately $7m in fines against Jetro's acquiring bank, PNC, which in turn withheld the same amount from Jetro. The court held that Jetro did not have a contract with Mastercard that allowed it to pursue claims against Mastercard, and in any case, Jetro had agreed that PNC could pass on any charges for PCI violations to Jetro.[25] A particularly alarming part of the court's decision for merchants was its response to Jetro's argument that Mastercard could essentially impose its requirements on the agreement between Jetro and PNC: 'If [Jetro] was not comfortable with the [PCI DSS], it could have elected to not accept MasterCard credit cards as a means for

customers to make payment at its stores. It could instead have to accept other credit cards only or not to accept credit cards at all.'[26] This is an indication that, at least in New York, courts may not be sympathetic to the criticisms that the payment card brands hold all of the power and can make decisions unilaterally.

Merchants have also sued acquirers about PCI enforcement. After Cisero's Ristorante and Nightclub in Park City, Utah (Cisero's) had funds confiscated from its bank account by its acquiring bank, U.S. Bank, Cisero's asserted claims against U.S. Bank and its payment processor, Elavon for, among other things, recovery of those seized funds.[27] Cisero's alleged that the bank confiscated funds following a supposed data breach even though an investigation found no evidence of a breach actually occurring. The lawsuit argued that U.S. Bank and the payment card industry in general compel merchants to sign one-sided contracts that are based on standards that change arbitrarily and without warning, impose whatever fines they see fit, even without proof of a breach or any economic loss, and do not provide merchants the opportunity to dispute claims before seizing funds as penalties.[28] The case was dismissed soon after Cisero's counterclaims were filed, likely because of a confidential settlement.[29]

In another case, *Schnuck Markets, Inc. v. First Data Merchant Servs. Corp.*,[30] Schnucks was breached, and its processor First Data began withholding a percentage each day from the funds it collected for transactions at Schnucks.[31] Schnucks alleged that the amount withheld by First Data exceeded the contractual limitation on liability in the parties' Master Services Agreement, and First Data argued that the agreement allowed it to withhold costs for all of the losses stemming from the data breach. The court held, and the Eighth Circuit affirmed, that the limitation on liability applied.[32] The decision turned, in part, on a contractual provision that increased the liability cap if Schnucks were not PCI compliant, which First Data did not allege.[33] In a related case, several issuers sued Schnucks for losses relating to the data breach. The district court dismissed the issuers' claims, and the Seventh Circuit affirmed, holding that the issuers 'and Schnucks all participate in a network of contracts that tie together all the participants in the card payment system.'[34] The issuers could not recover losses above and beyond the contractual damages simply 'because they are disappointed by the reimbursement they received through the contractual card payment systems they joined voluntarily.'[35]

Furthermore, although entities may use PCI compliance as evidence — but not proof — that it implemented a reasonable information security plan in litigation stemming from data breaches, even that benefit is limited. Non-compliance has been noted by courts as evidence that a company breached its duty of care.[36] And even if entities are PCI compliant, the FTC has stated that 'the existence of a PCI DSS certification is an important consideration in, but by no means the end of, our analysis of reasonable security'.[37]

But PCI compliance and enforcement also has its defenders. For example, Bruce Schneier, currently the Chief Technology Officer of IBM Resilient, fellow at Harvard University's Berkman Klein Center, and board member of the Electronic Frontier Foundation, called the PCI DSS 'the best stick the [payment card] industry has found to beat companies over the head with', saying that the PCI DSS 'forces companies to take security more seriously'.[38] To PCI defenders, if entities did not have severe consequences for failing to protect customer data, they would have no incentive to do so.

Key updates to PCI DSS in 2018

As mentioned above, the latest version of PCI DSS is 3.2 and organisations must implement all new requirements by 1st

February, 2018. New requirements are as follows:

For all organisations

- Change management processes to confirm that affected PCI DSS requirements are in place after significant change (Requirement 6.4.6);
- Multi-factor authentication for all non-console administrative access (Requirement 8.3.1).

Additional requirements for service providers

- Maintain a documented description of the cryptographic architecture (Requirement 3.5.1);
- Detect and respond to failures of critical security control systems (Requirements 10.8, 10.8.1);
- Perform penetration testing on segmentation controls at least every six months (Requirement 11.3.4.1);
- Establish a formal PCI DSS compliance program (Requirement 12.4.1);
- Perform reviews at least quarterly to ensure security policies and procedures are followed (Requirements 12.11, 12.11.1).

All organisations must also migrate out of the vulnerable version of SSL/TLS by 30th June, 2018. SSL/TLS is a cryptographic protocol used to establish a secure communication channel between two systems. There are known vulnerabilities with earlier versions of the protocol and, thus, why the Payment Card Industry is mandating upgrading to a more secure version.

CONCLUSION

Although there are some harsh criticisms of PCI DSS, all evidence points to it remaining in place for the foreseeable future. Professionals in all industries that accept, process, store or transmit credit card information need to be aware of and understand the requirements of the PCI DSS, not only to avoid the consequences of non-compliance, but to improve their security posture for not only cardholder data, but all forms of data. Because PCI compliance is a fairly new subject, there is plenty of room for it to change and grow. It is critical for professionals to keep up to date on the changing best practices, rules and requirements, and legal developments surrounding the PCI DSS.

References

1. PCI Security Standards Council (April 2016), 'Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures Version 3.2', p. 5, available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (accessed 17th April, 2018).
2. PCI Security Standards Council, available at https://www.pcisecuritystandards.org/ (accessed 17th January, 2018).
3. Visa, 'Receiving Payments' available at https://www.visaeurope.com/receiving-payments/security/ (accessed 3rd April, 2018); PCI DSS, 'Frequently Asked Questions', available at https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-PCI-DSS-a-global-standard (accessed 3rd April, 2018).
4. Visa and Mastercard require all payment processors, third-party agents/service providers to be registered. More information on Visa and Mastercard's registration programmes and list of compliant processors, third-party agents and service providers is available on their websites. Visa, available at https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html (accessed 19th January, 2018); Mastercard, available at https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/service-providers-need-to-know.html (accessed 19th January, 2018).
5. PCI Security Standards Council (May 2016), 'The Prioritized Approach to Pursue PCI DSS Compliance', available at https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf (accessed 17th January, 2018).
6. PCI Security Standards Council (May 2016), 'Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) v3.2', available at https://www.pcisecuritystandards.org/documents/PA-DSS-v3_2-Program-Guide.pdf?agreement=true&time=1515785992476 (accessed 17th January, 2018).

7. SecurityMetrics (2017), '2017 Guide to PCI DSS Compliance', available at https://www.securitymetrics.com/static/resources/orange/2017-securitymetrics-pci-guide.pdf (accessed 17th January, 2018).
8. Visa (October 2015), 'New Small Merchant Data Security Requirement', available at https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-10292015.pdf (accessed 17th January, 2018).
9. Visa (USA), https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-faq.pdf (accessed 3rd April, 2018).
10. PCI (October 2010), 'Data Security Standard', available at https://www.pcisecuritystandards.org/documents/pci_dss_emv.pdf (accessed 3rd April, 2018).
11. Visa, 'Data Security Compliance & PCI DSS Merchant Levels', https://usa.visa.com/support/small-business/security-compliance.html (accessed 17th January, 2018). See also American Express, 'American Express Data Security Requirements, United States, Puerto Rico, and the U.S. Virgin Islands', available at https://icm.aexp-static.com/Internet/NGMS/US_en/Images/DataSecurityRequirementsOptBlue.pdf (accessed 17th January, 2018); Mastercard, 'What Merchants Need to Know About Securing Transactions', available at https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html (accessed 17th January, 2018).
12. Visa (USA), 'What To Do If Compromised', available at https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf (accessed 17th January, 2018).
13. PCI Security Standards Council, 'About Us', https://www.pcisecuritystandards.org/about_us/ (accessed 17th January, 2018).
14. Minn. Stat. § 325E.64 (2007).
15. Nev. Rev. Stat. § 603A.215 (2009); Wash. Rev. Code § 19.255.020.
16. *Ibid*., note 2, Q15.
17. 'Do the Payment Card Industry Data Standards Reduce Cybercrime?: Hearing Before the H. Subcomm. On Emerging Threats, Cybersecurity, and Science and Technology of the H. Comm. On Homeland Security' (2009), 111th Cong. 35–36 (statement of Michael Jones, Chief Information Officer of Michaels' Stores).
18. *Ibid*., note 17, p. 41 (statement of David Hogan, Senior Vice President, Retail Operations, and Chief Information Officer for the National Retail Federation).
19. Jaikumar Vijayan (March 2009), 'Visa Drops Heartland, RBS WorldPay from PCI Compliance List After Breaches', Computerworld, available at https://www.computerworld.com/article/2531653/technology-law-regulation/visa-drops-heartland--rbs-worldpay-from-pci-compliance-list-after-breaches.html (accessed 17th January, 2018).
20. *Ibid*., note 19.
21. *Ibid*., note 19.
22. *Genesco Inc. v. Visa, Inc.*, No. 3:13-cv-00202, Complaint, ¶ 48 (Dkt.1) (M.D. Tenn., Mar. 7, 2013).
23. *Ibid*., note 22 (dismissed 3rd June, 2016).
24. Index No. 60374/2015, 51 Misc.3d 1217(A), 2016 WL 1761971 (Westchester Cty. Dec. 4, 2015).
25. *Ibid*., note 24, p. 10.
26. *Ibid*., note 24, p. 11.
27. Zetter, K. (January 2018), 'Rare Legal Fight Takes on Credit Card Company Security Standards and Fines', Wired, available at https://www.wired.com/2012/01/pci-lawsuit/ (accessed 17th January, 2018).
28. *Elavon, Inc. v. Cisero's, Inc. and Theodora McComb*, Civil No. 100500480, Amended Counterclaim (3rd Jud. Dist. Ct. Summit Cty., Aug. 8, 2011).
29. Goodman, E. (July 2015), 'Store's Data Breach Reveals Payment Card Liability Quandary', Business Insurance, available at http://www.businessinsurance.com/article/00010101/STORY/307059999/Stores-data-breach-reveals-payment-card-liability-quandary (accessed 17th January, 2018).
30. No. 4:13-cv-02226-JAR (E.D. Mo.).
31. *Ibid*., note 30, Substitute Complaint ¶ 31 (Dkt. 9).
32. *Ibid*., note 30, 86 F. Supp. 3d 1055 (E.D. Mo. 2015); *aff'd* 852 F.3d 732 (8th Cir. 2017).
33. *Ibid*., note 30, Order at 15–17.
34. *Cmty. Bank of Trenton, et al. v. Schnuck Mkts., Inc.*, No. 15-cv-01125-MJR, 2017 WL 1551330 (S.D. Ill. May 1, 2017); *aff'd* 887 F.3d 803, 814 (7th Cir. 2018).
35. *Ibid*., note 34, 887 F.3d at 815.
36. *Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 951–52 (S.D. Cal. 2012) ('[A]ccording to plaintiffs, Sony did nothing to update its inadequate protocols or otherwise implement adequate safeguards. … [T]his is further evidenced by Sony's decision not to install and maintain appropriate firewalls on its networks, including the [PCI DSS], which … is standard in the industry'.); *Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 526 (N.D. Ill. 2011) ('Plaintiffs allege that Michaels failed to comply … with the PCI Pin Security Requirements'.).
37. Federal Trade Commission, Statement of the Federal Trade Commission — *FTC v. LifeLock* (Dec. 17, 2015), https://www.ftc.gov/system/files/documents/public_statements/896143/151217lifelockcommstmt.pdf (accessed 17th January, 2018).
38. Mimoso, M. S. (January 2008), 'Bruce Schneier Reflects on a Decade of Security Trends', Schneier on Security, available at https://www.schneier.com/news/archives/2008/01/bruce_schneier_refle.html (accessed 17th January, 2018).