PAYMENT CARD FRAUD, DATA BREACHES, AND EMERGING PAYMENT TECHNOLOGIES

Salvatore Scanio
Jason W. Glasgow

I. INTRODUCTION

In today's cybercrime era, a cliché has evolved: there are two types of companies, those that have been hacked (or do not know that they have been) and those that will be hacked. The theft of payment cards is a top target in data breaches. Payment card fraud has been escalating, fueled by major data breaches involving millions of card numbers. Meanwhile, the payment card landscape is changing rapidly, with new technologies, designed to provide faster and safer transactions.

This article presents an overview of the evolving payment card system and nature of payment card fraud. It discusses current and developing loss allocation under federal law and card network rules, and how, in the event of payment card theft as a result of a data breach, loss allocation is being shifted in several developing areas, including consumer class action litigation, claims by issuing banks against merchants, and card network fines and assessments. The article then examines how emerging payment technologies, in the form of EMV chip-card technology, Near Field Communication, tokenization, and encryption, are being implemented in varying degrees. Finally, the article discusses the expected impact these technologies will have on payment card fraud.

Salvatore Scanio is a member of Ludwig & Robinson, PLLC in Washington, D.C. Jason W. Glasgow is CyberRisk Product Manager with Travelers in Hartford, Connecticut.

II.
AN OVERVIEW OF THE PAYMENT CARD SYSTEM

Electronic payment cards represent an important and growing role in the United States payments system. There were over 82 billion electronic payment card transactions in 2012, an increase from 35 billion in 2003,[1] doubling in total value from $2.33 trillion to $4.52 trillion.[2] Payment card transactions account for about 67 percent of the number but less than 3 percent of the value of all consumer and business noncash payments in the United States.[3] In recent years, "payments have become increasingly card-based,"[4] as card use has grown substantially, while check use has declined.[5] More than two-thirds of all consumer and business noncash payments were made with payment cards in 2012, increasing from 43 percent in 2003.[6]

The payment card system generally involves five parties. A "cardholder," typically a consumer, uses a payment card to make purchases at a merchant. An "issuer" is a financial institution that issues a payment card to the cardholder. The term "merchant" applies to any entity that accepts payment cards in exchange for goods or services. An "acquiring bank" is the merchant's bank or processing partner that processes card payments through "payment card networks" (*e.g.*, Visa, MasterCard).[7]

There are three types of payment cards: credit, debit, and prepaid. Credit cards are used to access lines of credit. Debit cards are

---

[1] BD. OF GOVERNORS OF THE FED. RESERVE SYS., THE 2013 FEDERAL RESERVE SYSTEM PAYMENTS STUDY: RECENT AND LONG-TERM PAYMENT TRENDS IN THE UNITED STATES: 2003-2012 7-8, 42 (rev. July 2014) [hereinafter BD. OF GOVERNORS].

[2] *Id*. at 42.

[3] *Id*. at 12, 41.

[4] *Id*. at 6.

[5] *Id*. at 12-13.

[6] *Id*. at 12.

[7] Julia S. Cheney, FEDERAL RESERVE BANK OF PHILA., HEARTLAND PAYMENT SYSTEMS: LESSONS LEARNED FROM A DATA BREACH, PAYMENT CARDS CENTER 1-2 (Jan. 2010), *available at* https://www.philadelphia-fed.org/consumer-credit-and-payments/payment cards-center/ (last visited Aug. 18, 2015).

linked directly to deposit or brokerage accounts. Prepaid cards, also known as stored-value cards, access funds in special purpose prepaid accounts.[8]

Payment card transactions may be classified into two general types. Card present or point-of-sale is used to denote transactions where the payment card is present. Conversely, card-not-present[9] signifies transactions where the payment card is not present, such as online or telephone transactions.[10]

The payment card transaction process has two major parts: authorization and clearing/settlement. Authorization takes place when information from the payment card is presented to the merchant for a purchase, either card present or card-not-present. Information from the card is obtained by swiping the card through a point-of-sale terminal or by manually entering the card data. The merchant electronically sends the card information and transaction amount to its processor/acquiring bank, which then sends an authorization request to the specific issuing bank through the applicable card network. The issuing bank verifies the card and amount, transmits a transaction approval or denial to the processor/acquiring bank, which then relays the response to the merchant.[11]

The clearing and settlement process takes place separately from the authorization of a specific transaction. The merchant sends its transactions to its processor/acquiring bank, which then distributes the transactions to the appropriate network (*e.g*. MasterCard transactions to the MasterCard network, etc.). The card networks serve as a clearinghouse for payments, in which funds are transferred from the issuer's account to the acquirer's account, minus an interchange fee. The

[8] BD. OF GOVERNORS, *supra* note 1, at 14.

[9] Hereinafter CNP.

[10] *Id*.

[11] Ramon P. DeGennaro, *Merchant Acquirers and Payment Card Processors: A Look Inside the Black Box*, FED. RES. BANK ATLANTA ECON. REV., 1Q2006, at 32-33.

acquirer then transfers funds to the merchant's account, less the acquirer's fees, and the issuing bank charges the cardholder.[12]

III.
PAYMENT CARD FRAUD

Historically, payment card fraud occurred when a card was lost or stolen and the card was taken to make unauthorized purchases. In the internet age, payment card fraud primarily occurs when *information* is stolen, rather than the physical card, usually through a data breach in which a payment card or personal information is misappropriated. A "specialized electronic payment fraud industry" has developed over the last decade as "criminals who were carrying out card fraud and attacks on electronic banking got organized, thanks to a small number of criminal organizations and a number of chat-rooms and other electronic fora, where criminals can trade stolen card and bank account data, hacking tools and other services."[13] Within this "fraud industry," different groups "specialize in activities such as writing malware, hacking databases, organizing underground electronic marketplaces, and laundering money."[14]

The most common source of card fraud is a hacked merchant in which malicious software is installed on a merchant's point-of-sale system, card information is stolen, and the thieves create counterfeit cards from the stolen data to make unauthorized purchases.[15] A recent trend has seen "a shift from a reliance on default credentials to the capture and use of stolen credentials. These are also not mere opportunistic attacks. Many incidents involved direct social engineering of store employees (often via a simple phone call) in order to trick them into providing the password needed for remote access to the POS."[16] A

---

[12] *Id*. at 33-34.

[13] Richard J. Sullivan, *The Changing Nature of U.S. Card Payment Fraud: Industry and Public Policy Options*, FED. RES. BANK. OF KANSAS CITY ECON. REV., 2Q2010, at 104.

[14] *Id*.

[15] Brian Krebs, *How Was Your Credit Card Stolen*?, KREBS ON SECURITY (Jan. 19, 2015), http://krebsonsecurity.com/2015/01/how-was-your-credit-card-stolen/ (last visited Aug. 14, 2015).

[16] VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT 36 (2015).

data breach may take place anywhere in the payment card processing stream, from the merchant's bank or payment processing company to a card issuer's bank, or via any third-party service company or vendor utilized by a merchant or bank.[17] Another form of card theft is "skimming," in which thieves place devices on ATMs or gas station pumps to capture card information and tiny cameras are used to steal personal identification numbers.[18] Card information may also be stolen from online merchant websites that have been hacked, from malware on a card user's computer on which the user has submitted card information, or by dishonest employees, such as restaurant workers, using a hidden or handheld device to copy card data.[19]

Cards held by both consumers and businesses are subject to theft. According to the Association of Finance Professionals, the "second most popular vehicle for payments fraud [of surveyed member companies] is corporate and commercial credit/debit cards. A third of finance professionals (34 percent) whose organizations were exposed to payments fraud in 2014 report that such fraud attempts were via credit/debit cards."[20]

In 2014, the total amount of direct payment card losses to criminals incurred by issuers, merchants, and acquirers, was estimated to be $16.31 billion worldwide, an increase of 19 percent over 2013, according to *The Nilson Report*, a payments industry newsletter.[21] In terms of the allocation of worldwide losses, issuers lost 62 percent, with merchants and acquirers accounting for the other 38 percent.[22] Of the $16.31 billion global loss, the United States accounted for 48 percent, while generating only 21 percent of total volume.[23] Thus, U.S. fraud was

[17] Krebs, *supra* note 15.

[18] Robin Sidel, *Theft of Debit-Card Data from ATMs Soars*, WALL ST. J., May 19, 2015, http://www.wsj.com/articles/theft-of-debit-card-data-from-atms-soars-1432078912 (last visited Aug. 26, 2015).

[19] Krebs, *supra* note 15.

[20] ASSOCIATION OF FINANCE PROFESSIONALS, 2015 PAYMENTS FRAUD AND CONTROL SURVEY 4 (Mar. 2015).

[21] THE NILSON REPORT, July 2015, at 5.

[22] *Id*. at 5.

[23] *Id*. at 11.

12.75 cents per $100 (or 12.75 basis points), while the rest of the world was only 3.73 cents per $100.[24]

According to the Federal Reserve System, there were 29.8 million fraudulent payment card transactions in the United States in 2012, with a fraud rate of 3.74 basis points (3.74 unauthorized transactions per 10,000 transactions).[25] Losses from card fraud totaled $4.1 billion, or about 8.43 basis points by card transaction value.[26] The difference between card-not-present and card-present fraud is significant. The 2013 Federal Reserve Payments Study concluded:

> Card-not-present third-party fraud rates for debit and general-purpose credit cards were estimated to have been approximately three times as likely to be unauthorized as their card-present counterparts: for credit cards, the estimated card-not-present fraud rate by number was 11.44 basis points compared with 3.92 basis points for card-present; for debit cards, the estimated card-not-present fraud rate by number was 10.10 basis points compared with 3.07 basis points for card-present.[27]

Global payment card fraud is expected to grow. In 2020, worldwide fraud losses are predicted to exceed $35.54 billion, with card fraud for 2015 through 2020 expected to total $189.29 billion.[28]

IV.
PAYMENT CARD FRAUD LIABILITY

Generally, the liability for payment card fraud does not fall on cardholders, especially consumers, but rather on issuers, acquirers, and merchants. The allocation of liability for payment card fraud mainly occurs through a combination of federal law and private arrangements,

[24] *Id.*
[25] BD. OF GOVERNORS, at 33, 43.
[26] *Id.*
[27] *Id*. at 35.
[28] THE NILSON REPORT, *supra* note 21, at 12.

primarily card-network rules, with various supplemental rules provided by state data breach notification laws.[29]

A. Federal Law Limitations on Consumer Liability for Payment Card Fraud

Federal law generally limits individual consumer liability for unauthorized credit and debit card transactions to $50, under differing circumstances. For credit cards, governed by the Truth in Lending Act and Regulation Z, a consumer's liability is limited to $50, with no liability for any unauthorized transaction after notice to the card issuer of the loss, theft, or possible unauthorized use of the card.[30] The burden of proof is on the card issuer to show that the use was authorized.[31]

For debit cards, governed by the Electronic Funds Transfer Act and Regulation E, a consumer's liability is also generally limited to $50, provided notice is given to the card issuer within two business days after learning of the loss or theft of the card.[32] A consumer's liability for unauthorized debit card use may increase to a maximum of $500 if the

[29] One key example is Minnesota's Plastic Security Card Act, discussed below. For a discussion of state data breach notification laws, see generally Rachael M. Peters, *So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Law*, 56 ARIZ. L. REV. 1171 (2014); Paul M. Schwart & Edward J. Janer, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007). Forty-seven states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands "have enacted legislation requiring private or government entities to notify individuals of security breaches of information involving personally identifiable information." NAT'L CONF. OF ST. LEGISLATURES, *Security Breach Notification Laws*, Jun. 11, 2015, http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Aug. 17, 2015). In view of varying state data breach notification laws, the Obama Administration in early 2015 proposed a national data breach notification law, the Personal Data Notification & Protection Act. THE WHITE HOUSE, *Fact Sheet: Safeguarding American Consumers & Families*, Jan. 12, 2015, https://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families (last visited Aug. 19, 2015).

[30] 15 U.S.C. § 1643(a); 12 C.F.R. § 226.12(b).

[31] 15 U.S.C. § 1643(b).

[32] 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(1).

consumer provides notices after two business days but within 60 days of the transmittal of the statement on which the unauthorized transaction appears, and the card issuer establishes that the transaction would not have occurred had there been timely notice.[33] If a consumer does not report unauthorized debit card use within 60 days of transmittal of the statement on which the unauthorized transaction appears, the consumer is exposed to unlimited liability if the card issuer establishes that the transaction would not have occurred if timely notice were given.[34] A card issuer must extend the two business day and 60-day time limits by a reasonable period when the consumer's delay in providing notice was due to extenuating circumstances.[35] In all events, when a consumer reports unauthorized debit card use, the burden of proof is on the card issuer to show the transaction was authorized.[36]

Unlike credit and debit cards, prepaid cards generally have not been subject to the same federal laws providing consumer liability limits for unauthorized use. The exceptions are reloadable payroll card accounts and government benefits cards, which are subject to the same liability limitations as debit cards.[37] The new Bureau of Consumer Financial Protection,[38] however, has issued proposed rules to generally treat prepaid cards like debit cards for purposes of consumer liability for unauthorized transactions.[39] Under the CFPB's proposal, prepaid cards with overdraft services and other credit features would be treated in the same way as credit cards for purposes of fraud liability.[40]

Also unlike cards issued to consumers, business cardholders are not subject to the same liability limitations for unauthorized card use. Businesses generally are excluded from coverage under the Truth in Lending Act and Electronic Funds Transfer Act, and therefore the various liability limitations for fraudulent credit and debit transactions do

[33] 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(2).
[34] 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(3).
[35] 15 U.S.C. § 1693g(a); 12 C.F.R. § 205.6(b)(4).
[36] 15 U.S.C. § 1693g(b).
[37] *See* 12 C.F.R. §§ 205.15, 205.18.
[38] Hereinafter CFPB.
[39] *See* 79 Fed. Reg. 77,102 (2014) (to be codified at 12 C.F.R. pts. 1005 and 1026) (proposed Dec. 23, 2014).
[40] *Id*.

not apply to cards issued to businesses.[41] Business cardholders, however, have fraud liability protections provided by their card issuers, as next discussed.

B. Card Network Liability Rules

The rules of the payment card networks play an important role in allocating liability among participants. Card issuers and acquirer banks, as members of the card networks, are bound by the rules of the respective networks (*e.g.*, Visa, MasterCard). Acquirers then apply the network rules to merchants through their contracts with merchants.

Cardholders are also impacted by the rules of the payment card networks. For example, both MasterCard and Visa have "zero liability" policies for consumer and business cardholders of credit and debit cards, as well as certain prepaid cards. These policies generally require the cardholder to have acted with reasonable care and to have reported the lost or stolen card promptly to the issuer.[42]

---

[41] *See* 15 U.S.C. § 1603 (the Truth in Lending Act exempts "extensions of credit primarily for business, commercial, or agricultural purposes, or to governmental agencies or instrumentalities, or to organizations"); 15 U.S.C. § 1693a (the Electronic Funds Transfer Act defines "account" as one "established primarily for personal, family, or household purposes").

[42] *See* MASTERCARD, *Zero Liability Protection*, https://www.mastercard.us/en-us/about-mastercard/what-we-do/terms-of-use/zero-liability-terms-conditions.html (last visited Aug. 14, 2015) ("As a MasterCard cardholder, zero liability applies to your purchases made in the store, over the telephone, online, or via a mobile device. As a cardholder, you will not be held responsible for unauthorized transactions if: 1. you have used reasonable care in protecting your card from loss or theft; and 2. you have promptly reported to your financial institution when you knew that your MasterCard was lost or stolen."); VISA, *Zero Liability Policy*, http://usa.visa.com/personal/security/zero-liability.jsp (last visited Aug. 14, 2015) ("If the unauthorized transaction involves your debit card or account, Visa's Zero Liability Policy requires issuers to replace any funds taken from your account as the result of an unauthorized debit transaction within 5 business days of notification. In the event you experience unauthorized transactions: Notify your financial institution immediately of any unauthorized use. Replacement funds are provided on a provisional basis and may be withheld, delayed, limited, or rescinded by your issuer based on the following: Gross negligence or fraud; Delay in reporting unauthorized use; Investigation

In allocating liability for fraudulent payment card transactions among issuers and acquirers, the payment card networks have substantially similar rules.[43] Generally, for card-present transactions, where a signature is obtained or PIN code is used and the card itself may be examined, the issuer is subject to liability for unauthorized transactions, provided the merchant followed required security steps.[44] These steps typically involve inspecting the card, obtaining authorization from the issuer and a signature from the cardholder.[45] Card issuer losses for card-present transactions occur mainly from counterfeit cards used in fraudulent transactions for which issuers have given merchants authorization.[46]

For card-not-present transactions, the acquirer generally bears liability for unauthorized transactions, which then passes the loss to the merchant.[47] Acquirer/merchant losses "occur mainly on card-not-present (CNP) transactions on the Web, at a call center, in a mobile app, or through mail order because issuers can charge back fraudulent transactions when plastic cards have not been read by a terminal…."[48]

C. Payment Card Industry Data Security Standard

About ten years ago, the card networks created the Payment Card Industry Security Standard Council to promulgate non-binding data security standards for payment cards "to mitigate data breaches and

---

and verification of claim; Account standing and history."). *See also* VISA, *Zero Liability*, http://usa.visa.com/small-business/card-benefits/security/zero-liability.jsp (last visited Aug. 14, 2015) (applying zero liability to business cardholders).

[43] *See, e.g.*, MASTERCARD, MASTERCARD RULES (Dec. 11, 2014); VISA, VISA CORE RULES AND VISA PRODUCT AND SERVICE RULES (Apr. 15, 2015).

[44] *See* Paycom Billing Servs., Inc. v. MasterCard Int'l, Inc., 467 F.3d 283, 286-88 (2d Cir. 2006); Adam J. Levitin, *Private Disordering? Payment Card Fraud Liability Rule*, 5 BROOK. J. CORP. FIN. & COM. L. 1, 15 (2010).

[45] Levitin, *supra* note 44, at 15.

[46] THE NILSON REPORT, *supra* note 21, at 10.

[47] *See* Paycom Billing Servs., Inc., 467 F.3d at 286-88; Levitin, *supra* note 44, at 1, 15.

[48] THE NILSON REPORT, *supra* note 21, at 10.

prevent payment cardholder data fraud."[49] The PCI SCC is owned by the five major card networks (American Express, Discover Financial Services, JCB International, MasterCard, and Visa, Inc.).[50] The PCI SCC also has approximately 700 "participating organizations," including merchants, financial institutions, processors, trade associations, point-of-sale providers, and others to provide "input to the organization and feedback on the evolution of the PCI standards."[51]

The PCI Data Security Standard is based on twelve basic requirements, as follows:[52]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**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 cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware 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.** Identify and authenticate access to system components **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 addresses information security for all personnel

[49] PAYMENT CARD INDUSTRY SECURITY STANDARD COUNCIL, *About the PCI Security Standards Council*, https://www.pcisecuritystandards.org/organization_info/index.php (last visited Aug. 19, 2015) [hereinafter PCI SCC].

[50] *Id.*

[51] PAYMENT CARD INDUSTRY SECURITY STANDARD COUNCIL, *Organizational Structure*, https://www.pcisecuritystandards.org/organization_info/org_fact_sheet.php (last visited Aug. 19, 2015); PAYMENT CARD INDUSTRY SECURITY STANDARD COUNCIL, *Participating Organization*, *available at* https://www.pcisecuritystandards.org/get_involved/member_list.php (last visited Aug. 19, 2015).

[52] Hereinafter PCI DSS. *See* PAYMENT CARD INDUSTRY SECURITY STANDARD COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES VERSION 3.1 5 (Apr. 2015), *available at* https://www.pcisecuritystandards.org/security_standards/index.php (last visi-ted Aug. 28, 2015).

Each of these twelve requirements is detailed with numerous sub-requirements in the PCI's latest *Data Security Standard*: *Requirements and Security Assessment Procedures Version 3.1*, published in April 2015.[53] In addition, there are separate requirements to validate compliance through self-assessments.[54]

The PCI SCC does not enforce its standards. Rather, the card networks enforce the PCI DSS through their network agreements requiring participants to be PCI DSS compliant.[55] The card networks enforce PCI DSS compliance through the imposition of fines and penalties, as well as liability shifting, as discussed below. The PCI's standards have not been without controversy, as merchant groups have contended that the PCI DSS is aimed at protecting the interests of card networks and issuers, while imposing compliance costs on processors and merchants and, in some instances, unworkable rules.[56]

Industry compliance with PCI DSS is incomplete but improving. According to Verizon's *2015 PCI Compliance Report*, 20 percent of the companies tested were fully compliant with PCI DSS's 12 requirements in 2014, a substantial increase from only 11.1 percent in 2013.[57] Larger merchants are more likely to be in compliance with PCI DSS, with smaller merchants lagging. According to Visa, as of December 31, 2014, 97% of Visa's largest merchants in the United States, representing 50% of Visa's transactions, had validated their compliance with PCI DSS, and 88% of the next largest merchants with over one million in Visa transactions had validated compliance.[58] The compliance level for Visa's

[53] *Id.*

[54] *Id*. at 17.

[55] *E.g*., VISA, *supra* note 43, at CR-76-77, CR-84-85, PSR-277, PSR-480, PSR-486.

[56] Sullivan, *supra* note 13, at 119-204.

[57] VERIZON ENTERPRISE SOLUTIONS, VERIZON 2015 PCI COMPLIANCE REPORT 2 (Mar. 24, 2015).

[58] VISA, *U.S. PCI DSS Compliance Status*, Dec. 31, 2014, *available at* http://usa.visa.com/download/merchants/cisp-pcidss-compliancestats.pdf (last visited Aug. 19, 2014).

merchants with less than one million transactions, however, was "moderate" or 67%.[59]

Addressing the relationship between PCI DSS compliance and the incidence of a data breach, Verizon's *2015 PCI Compliance Report* observed: "Of all the data breaches that our forensics team has investigated over the last 10 years, not a single company has been found to be compliant at the time of the breach—this underscores the importance of PCI DSS compliance."[60] PCI compliance, however, does not mean that compliant firms are not susceptible to data breaches.[61] For example, several data breaches have taken place at retailers and processors that purportedly were PCI compliant.[62]

V.
DATA BREACHES AFFECTING PAYMENT CARDS

For the last several years, data breaches have become an everyday phenomenon. According to Verizon's *2015 Data Breach Investigations Report*, across all industries worldwide in 2014, there were 79,790 security incidents, with 2,122 breaches involving a confirmed data loss, and 700 million compromised records.[63] This

[59] *Id.*

[60] VERIZON ENTERPRISE SOLUTIONS, *supra* note 58, at 3. *See also* VERIZON, 2012 DATA BREACH INVESTIGATIONS REPORT 3 (2012) (in 2011, 96% of firms suffering a data breach had not achieved PCI DSS compliance).

[61] VERIZON ENTERPRISE SOLUTIONS, *supra* note 58, at 14 ("One of the criticisms of the PCI DSS, in common with any set of standards, is that focusing on compliance validation could actually be a distraction from achieving and maintaining genuine security. But for most companies the DSS provides a useful baseline. While validation is no assurance of security, not being compliant is pretty much a guarantee that you're not secure.").

[62] Sullivan, *supra* note 13, at 119; Avivah Litan, *How PCI Failed Target and U.S. Consumers*, GARTNER BLOG NETWORK, Jan. 20, 2014, http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/ (last visited Aug. 19, 2015); Jaikumar Vijayan, *After Target, Neiman Marcus Breaches, Does PCI Compliance Mean Anything?*, COMPUTERWORLD, Jan. 24, 2014, http://www.computerworld.com/article/2486879/data-security/after-target--neiman-marcus-breaches--does-pci-compliance-mean-anything-.html (last visited Aug. 19, 2015).

[63] VERIZON, *supra* note 16, at 3.

represents an increase from 63,000 security incidents in 2013, with 1,367 confirmed data breaches.[64] Payment card data is a top data breach target. In 2013, 41 percent of data breach victims had a credit card number compromised and 21 percent had a debit card number stolen.[65] Recent data breaches involving theft of payment card records from merchants include Home Depot (2014, 56 million payment cards) and Target (2013, 40 million payment cards), among numerous other companies.[66]

Large scale data breaches have also occurred at payment acquirers/processors where millions of payment card transactions are handled, such as the Heartland Payment System breach in 2008 involving 130 million records.[67] In addition, data breaches at nonfinancial firms, such as health insurers, universities, and government agencies, in which personal identity data is stolen, may result in payment card fraud. Fraudsters use the stolen information to commit identity theft by taking over a victim's payment card account or opening new payment card accounts in the victim's name.[68]

In addition to direct losses from payment card fraud discussed above, firms that suffer data breaches incur substantial indirect losses in the form of forensic experts, investigation costs, credit monitoring services, notification costs, and loss of business.[69] According to the Ponemon Institute's *2015 Cost of Data Breach Study*, the average cost of

---

[64] VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 2 (2014).

[65] LEXISNEXIS, 2014 LEXISNEXIS TRUE COST OF FRAUD STUDY 16 (2014).

[66] *See, e.g.*, Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES, Jan. 13, 2015, http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/ (last visited Aug. 26, 2015); PRIVACY RIGHTS CLEARINGHOUSE, *Chronology of Data Breaches*, https://www.privacyrights .org/data-breach (last visited Aug. 15, 2015).

[67] In re Heartland Payment Systems, Inc. Customer Data Security Breach Lit., 851 F. Supp. 2d 1040, 1047 & n.2 (S.D. Tex. 2012); Julia S. Cheney, *et al*., FED. RES. BANK OF PHILA., THE EFFICIENCY AND INTEGRITY OF PAYMENT CARD SYSTEMS: INDUSTRY VIEWS ON THE RISKS POSED BY DATA BREACHES 10-11 (Oct. 2012); *see generally* Cheney, *supra* note 7.

[68] Cheney, et al., *supra* note 67, at 11.

[69] According to an admittedly "very imprecise estimate," the "indirect costs of payment card compromised in 2011 might be as high as $1 billion." Cheney, et al., *supra* note 67, at 10.

a data breach in the United States was $217 per compromised record, representing a steady increase from $201 in 2014 and $188 in 2013.[70] Verizon recently developed a competing cost-of-data-breach model based on an analysis of 191 cyber liability insurance claims, finding the average cost per record in 2014 was only 58 cents, as compared to Ponemon's $201 estimate.[71] The Verizon model accounts for the fact that the cost of each stolen record is impacted by the total number of records compromised.[72] For example, the model predicts that the cost of a breach involving one million records will be between $892,400 and $1.8 million (95 percent of the time), and depending on circumstances could range up to as much as $27.5 million.[73] For breaches with 10 million records, the cost is estimated to fall between $2.1 million and $5.2 million (95 percent of the time), but could be as high as $73.9 million.[74]

VI.
DATA BREACH LIABILITY

A. Consumer Litigation

Major payment card data breaches usually are followed by consumer class-action litigation. Plaintiffs in class actions against merchants or card processors for failing to secure their confidential information allege various legal theories: negligence, breach of express or implied contract, violation of consumer protection laws, unfair competition, bailment, and invasion of privacy.[75]

The first and key issue that arises in data breach actions is standing. Under Article III of the Constitution, a plaintiff must have standing to sue to satisfy its "case or controversy" requirement. In order

---

[70] PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 2, 5 (May 2015), *available at* https://securityintelligence.com/media/2015-ponemon-cost-of-a-data-breach-study/#.VdM_f2dREdU (last visited Aug. 18, 2015).

[71] VERIZON, *supra* note 16, at 27.

[72] *Id.* at 27-30.

[73] *Id*. at 30.

[74] *Id*.

[75] John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 200 (2013).

to have standing, a plaintiff must have an actual or imminent injury in fact,[76] which may not be "too speculative."[77] While "allegations of possible future injury are not sufficient," an allegation of future harm can establish standing if that harm is "certainly impending."[78] Similarly, a "substantial risk" of harm may be sufficient, for as the U.S. Supreme Court has noted: "Our cases do not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[79]

In data-breach cases, the courts have split on the issue of whether the potential harm of identity theft is sufficient to confer standing. The First and Third Circuits, and district courts in other circuits, have held that a risk of future harm alone stemming from a data breach is insufficient to confer standing.[80] By contrast, the Seventh, Ninth, and

[76] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992).

[77] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).

[78] *Id*. (citations omitted).

[79] *Id*. at 1150 n.5 (2013) (citations omitted).

[80] Katz v. Pershing, LLC, 672 F.3d 64, 78 (1st Cir. 2012) (plaintiff incurred credit-monitoring services over concerns insecurely stored data could be hacked, but did not allege information was actually accessed); Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) (plaintiffs alleged risk of identity theft and credit monitoring costs following data breach at payroll processing firm); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876 (N.D. Ill. 2014) ("Whether [plaintiff] or other class members actually become victims of identity theft as a result of the data breach depends on a number of variables, such as whether their data was actually taken during the breach, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded."); Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646, 654-55 (S.D. Ohio 2014) ("Plaintiffs' allegation that Defendant offered a free year of credit monitoring and identity theft protection further supports the Court's conclusion that risk of injury is not certainly impending. Thus, Named Plaintiffs failed to allege facts demonstrating the increased risk makes any future injury 'certainly impending' as opposed to speculative.")

Eleventh Circuits, as well as other courts, have held the threat of identity theft sufficient for standing.[81]

Recently in *Remijas v. Neiman Marcus Group, LLC*,[82] the Seventh Circuit reversed a dismissal for lack of standing in a data-breach class-action suit. Retailer Neiman Marcus suffered a data breach in which 350,000 payment cards were exposed, of which 9,200 were known to have been used fraudulently.[83] Plaintiffs alleged that their damages included "lost time and money" in "resolving the fraudulent charges" and in "protecting themselves against future identity theft," and they also asserted that they were at an "increased risk of future fraudulent charges and greater susceptibility to identity theft."[84] Addressing the plaintiffs who acknowledged they had been reimbursed for known fraudulent charges and not suffered any identity theft, the Seventh Circuit held: "Those victims have suffered the aggravation and loss of value of the time needed to set things straight, to reset payment associations after credit card numbers are changed, and to pursue relief for unauthorized

[81] Resnick v. AvMed, Inc., 693 F.3d 1317, 1322-23 (11th Cir. 2012) (stolen information was used to open bank accounts in plaintiffs' names and make unauthorized purchase); Krottner v. Starbucks Corp., 628 F.3d 1139, 1141-43 (9th Cir. 2010) (suit by employees over theft of company laptop containing social security numbers, names, and addresses, in which future credit-monitoring expenses and "generalized anxiety and stress" were alleged damages); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 631-34 (7th Cir. 2007) (plaintiffs incurred credit-monitoring expenses following a data breach at online banking website); In re Target Corp. Cust. Data Sec. Breach Litig., No. 14-2522, 2014 U.S. Dist. LEXIS 175768, at *6-7 (D. Minn. Dec. 18, 2014) (finding standing sufficiently alleged for "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees"); Moyer v. Michaels Stores, Inc., No. 14 c 561, 2014 U.S. Dist. LEXIS 96588, at *19 (N.D. Ill. July 14, 2014) ("elevated risk of identity theft stemming from the data breach at Michaels is sufficiently imminent to give Plaintiffs standing"); In re LinkedIn User Privacy Litig., 2014 U.S. Dist. LEXIS 42696, at *15-16 (N.D. Cal. Mar. 28, 2014) (finding standing based on allegation plaintiff's "payment or overpayment was caused by LinkedIn's alleged misrepresentations, which she alleges she read and relied on in making her decision to purchase a premium subscription.").

[82] No. 14-3122, 2015 U.S. App. LEXIS 12487 (7th Cir. July 20, 2015).

[83] *Id.* at *3.

[84] *Id*. at *7-8.

charges."[85] Similarly, for customers whose stolen payment card had not been used, the court ruled they "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur."[86] The Seventh Circuit also rejected the argument that future harm was too speculative when Neiman Marcus itself recognized a substantial risk of harm in offering customers one year of credit monitoring and identity theft protection.[87]

Once standing is established, a second issue in data breach class actions is whether plaintiffs have viable causes of action, and a related third issue is damages. In *Anderson v. Hannaford Brothers Co*.,[88] a class action arising from the theft of 4.2 million payment cards at a grocery store chain, the only claims that survived dispositive motions were negligence and breach of implied contract, with damages limited to mitigation costs, *e.g*., fees for replacement cards and credit-monitoring expenses.[89] Some courts have applied the "economic loss doctrine" in negligence cases to preclude economic damages unless accompanied by non-economic injury. Under the economic-loss doctrine, courts have dismissed negligence claims in data breach cases, as out-of-pocket damages typically only involve credit monitoring expenses.[90]

A fourth issue in data-breach class actions is class certification. Under Fed. R. Civ. P. 23(a), four elements are required to certify a class:

---

[85] *Id*. at *8.

[86] *Id*. at *11-12 (citing Clapper, 133 S. Ct. at 1147).

[87] *Id*. at 14. The Seventh Circuit also noted " that these allegations go far beyond the complaint about a website's publication of inaccurate information, in violation of the Fair Credit Reporting Act, that is before the Supreme Court in *Spokeo, Inc. v. Robins*, No. 13-1339, *cert. granted* 135 S. Ct. 1892, 191 L. Ed. 2d 762 (2015)." *Id*. at *7-8.

[88] 659 F.3d 151 (1st Cir. 2011).

[89] 659 F.3d at 162-67.

[90] In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 498-99 (1st Cir. 2009); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E.2d 36, 46-47 (Mass. 2009); In re Target Corp. Cust. Data Sec. Breach Litig., 2014 U.S. Dist. LEXIS 175768, at *40-52 (D. Minn. Dec. 18, 2014) (conducting 11-state analysis); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 960-62 (S.D. Cal. 2012); Pa. State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 330 (M.D. Pa. 2005).

(1) numerosity, (2) commonality, (3) typicality, and (4) adequacy. Numerosity is met when "the class is so numerous that joinder of all members is impracticable."[91] In *In re Hannaford Brothers Co. Customer Data Securities Breach Litigation*,[92] the court certified a class consisting of customers who spent money on replacement cards and/or purchased credit monitoring or identity theft insurance, estimated to be 31,000 cardholders.[93] The court, however, expressed concern that few class members would actually be interested in filing a claim, citing *In re Heartland Payment Systems, Inc. Customer Sec. Breach Litigation*,[94] in which only 290 persons filed claims in a data breach involving 130 million potential class members, and, of those, only 11 claims were valid.[95]

In March 2015, a preliminary settlement was announced in the consumer class action in *In re Target Corp. Customer Data Security Breach Litigation*[96] The court certified a class for settlement purposes of "all persons in the United States whose credit or debit card information and/or whose personal information was compromised as a result of the data breach that was first disclosed by Target on December 19, 2013."[97] The settlement provides a $10 million fund for consumer compensation, for which each claimant is eligible up to $10,000. In order to recover, "victims must prove, among other things, that unauthorized charges were made to their credit cards. They must also show that they invested time in addressing the fraudulent charges and incurred costs from correcting their credit report because of higher interest rates or fees, from replacing driver's licenses or other forms of identification, or from hiring identity protection companies or lawyers."[98] Claimants may also receive

[91] Fed. R. Civ. P. 23(a)(1).

[92] 293 F.R.D. 21, 2013 U.S. Dist. LEXIS 39055 (D. Me. Mar. 20, 2013).

[93] *Id.* at *24-26.

[94] 851 F. Supp. 2d 1040, 1047 & n.2, 1050 (S.D. Tex. 2012).

[95] No. 2:08-MD-1954, 2013 U.S. Dist. LEXIS 39055, at *26.

[96] No. 0:14-MD-02522 (D. Minn.).

[97] Mar. 19, 2015 Order at 2, In re Target Corp. Cust. Data Sec. Breach Litig. (No. 0:14-MD-02522 D. Minn.).

[98] Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, N.Y. TIMES, Mar. 19, 2015, http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0 (last visited Aug. 17, 2015).

compensation for lost time, calculated at $10 per hour, for up to two hours for each type of substantiated loss.[99]

B. Claims By Issuing Banks Against Merchants

Like consumer class actions following major data breaches, issuing banks have also sought to bring class action suits against merchants. Because issuing banks generally are required to reimburse cardholders for fraudulent card-present transaction, they have attempted to shift their losses to merchants for failing take reasonable measures to protect payment card data, as required by industry standards. The issuing banks have also sought to recover other losses, such as the cost of reissuing cards and having to investigate and process fraud claims and other time-consuming activities. As a result of the Target data breach, the cost of reissuing cards alone was estimated to be $200 million.[100]

Issuing banks have brought claims against merchants (and in some cases the merchant's acquirer/processor) under various legal theories: negligence, negligent misrepresentation, breach-of-contract/third-party beneficiary, violation of state data protection statutes, and unfair competition. Like consumer class actions against merchants, claims by banks face similar or greater obstacles, including standing and viable causes of action.[101] For example, tort claims have been dismissed under the economic-loss doctrine.[102] On breach-of-contract claims, the courts have reached different conclusions. Issuing

[99] Mar. 19, 2015 Order at 2, In re Target Corp. Cust. Data Sec. Breach Litig. (No. 0:14-MD-02522 D. Minn.); Mar. 18, 2015 Settlement Agreement and Release, Distribution Plan, Doc. 358-1, at ¶ 1.1.2, In re Target Corp. Cust. Data Sec. Breach Litig. (No. 0:14-MD-02522 D. Minn.).

[100] Tim Sablik, *Cyberseuring Payments: Are we losing the Fight Against Next-Gen Bank Robbers?*, ECON. FOCUS, 1Q2014, at 15.

[101] *See, e.g.*, Mike Cherney, *TJX Cos., Banks Settle Class Action Over Data Breach*, LAW360, Sept. 2, 2009, http://www.law360.com/articles/120358/tjx-cos-banks-settle-class-action-over-data-breach (last visited Aug. 20, 2015) (four remaining banks settled with TJX for $525,000).

[102] *See, e.g.*, In re TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 499 (1st Cir. 2009); Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F.3d 162, 175-78 (3d Cir. 2008); CUMIS Ins. Society, Inc. v. BJ's Wholesale Club, Inc., No. 05-1158, 2005 Mass. Super. LEXIS 696, at *12-15 (Mass. Sup. Ct. Dec. 7, 2005).

banks have alleged that they were third-party beneficiaries to the contracts between the merchant and acquirer/processor, requiring the merchant to follow certain security practices and standards to protect payment card data pursuant to card-network rules. In *Sovereign Bank v. BJ's Wholesale Club, Inc.*,[103] the Third Circuit recognized a breach-of-contract claim, relying on a card network memorandum providing: "To protect the Visa system and *Issuers* from potential fraud exposure *created by databases of magnetic-stripe information.* . . . Acquirers are obligated to ensure that their merchants do not store the magnetic-stripe information from Visa Cards for any subsequent use."[104] In *In re TJX Cos. Retail Security Breach Litigation*,[105] the First Circuit dismissed a similar claim because later editions of the card-network rules contained provisions stating there was to be no third-party beneficiary of the contract.[106]

Recent suits by banks against Target and Home Depot stemming from data breaches are pending.[107] One key development impacting these suits has been the passage in recent years of various state data-protection statutes. For example, in *In re Target Corp. Customer Data Security Breach Litigation*,[108] the banks claimed that Target violated Minnesota's Plastic Security Card Act, providing:

> No person or entity conducting business in Minnesota that accepts [a payment card] in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

---

[103] 533 F.3d 162 (3d Cir. 2008).

[104] *Id*. at 173 (emphasis in original).

[105] 564 F.3d 489 (1st Cir. 2009).

[106] *Id*. at 499.

[107] In re Target Corp. Cust. Data Sec. Breach Litig., 64 F. Supp. 3d 1304 (D. Minn. 2014); May 27, 2015 Financial Institution Plaintiffs' Consolidated Class Action Complaint, In re Home Depot, Inc. Cust. Data Sec. Breach Litig. (No. 1:14-MD-02583 N.D. Ga.).

[108] 64 F. Supp. 3d 1304.

. . . .

> Whenever there is a breach of the security of the system of a person or entity that has violated this section . . . that person or entity shall reimburse the financial institution that issued any [payment cards] affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders . . . .[109]

The plaintiff banks alleged four causes of action against Target: (1) negligence in failing to provide sufficient security to prevent hackers from accessing customer data; (2) violations of Minnesota's Plastic Security Card Act;[110] (3) negligence per se based on violation of the PSCA; and (4) negligent misrepresentation by omission in failing to inform the banks of its insufficient security.[111] The district court rejected Target's motion to dismiss, except as to the negligent misrepresentation claim, which was dismissed without prejudice because the plaintiffs failed to plead reliance.[112]

C. Card Network Fines and Loss-Allocation Assessments

The card networks enforce compliance with the PCI Data Security Standard. One key method the card networks employ is the use of fines and loss allocation assessments for PCI non-compliance and data breach fraud losses under their operating rules via agreements with members. Acquiring banks/processors members then pass on applicable liability to merchants through their merchant processing agreements under indemnification clauses or other provisions.

---

[109] Minn. Stat. § 325E.64, subd. 2, 3. For a criticism of the Minnesota statute, see Richard A. Epstein and Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203, 221-23 (2008) (arguing payment card losses should be allocated solely through private ordering).

[110] Hereinafter PSCA.

[111] *In re Target Corp. Cust. Data Sec. Breach Litig.*, 64 F. Supp. at 1308.

[112] *Id.* at 1314.

Under the card-network rules, acquirers must ensure that its merchants are compliant with the PCI Data Security Standard.[113] To validate compliance, merchants generally must have annual PCI DSS assessments and quarterly network scans performed on their websites.[114] In the event of noncompliance, merchants are subject to fines by each of the card networks, in amounts ranging from $10,000 for a first violation to $200,000 for a fourth violation in the same calendar year.[115] In the of the event of a payment card data breach, merchants are subject to additional fines by each of the card networks, such as $100,000 for each violation of a PCI SCC requirement and $25,000 per day for each day the merchant is noncompliant.[116]

Beyond fines, the card networks have loss-allocation programs to shift certain losses from issuers to acquirers (and then to merchants) in the event of a payment card data breach "when there is a violation involving non-compliance with . . . . Payment Card Industry Data Security Standard [or other network rules] that could have allowed an Account Data Compromise Event."[117] Under card-network loss-allocation programs, an assessment for counterfeit fraud losses incurred by issuers and related operating expenses may be made against the responsible merchant for data breaches above certain sizes, such as 30,000 or more stolen cards and $300,000 or more in fraud losses.[118] Counterfeit fraud recovery assessments are generally calculated based on fraudulent transactions associated with the stolen cards.[119] Operating expense recovery assessments are "intended to offset a portion of estimated issuer expenses used for preventing, monitoring, blocking, and

[113] *E.g.*, MASTERCARD, SECURITY RULES AND PROCEDURES (MERCHANT EDITION) 89 (Feb. 5, 2015).

[114] *Id.* at 90-94.

[115] *Id.* at 94; *see also* WELLS FARGO, *Data Security/PCI Mandatory Compliance Programs*, https://www.wellsfargo.com/biz/merchant/service/manage/risk/security (last visited Aug. 25, 2015).

[116] *E.g.*, MASTERCARD, *supra* note 113, at 82, 88.

[117] *See* VISA, VISA GLOBAL COMPROMISED ACCOUNT RECOVERY GUIDE 1 (Jan. 2015). For MasterCard's similar program, see MASTERCARD, ACCOUNT DATA COMPROMISE USER GUIDE 6-1 to 6-14 (Jun. 26, 2014).

[118] VISA, *supra* note 117, at 4.

[119] *Id.*

reissuing affected accounts."[120] Visa's operating expense assessment is $2.50 per card. *Id.*

In large data breaches, the amounts of counterfeit fraud and operating expense recovery assessments may be significant. Recently, Target announced it would pay Visa $67 million for such assessments, and was working on resolving its assessment liability to MasterCard.[121] In 2010, Heartland Payment Systems paid Visa and MasterCard $100 million for its 2008 data breach.[122]

Some merchants have also attempted court challenges to card networks' loss allocation assessments. In *Genesco, Inc. v. VISA U.S.A., Inc.*,[123] a merchant was subjected to $13 million in counterfeit fraud and operating expense assessments and $10,000 in fines following a cyberattack on the merchant's computer network allowing payment card data to be stolen during the data-transmission process.[124] The merchant challenged the card network's finding that it violated PCI DSS, contending it was in compliance with applicable requirements at the time of the data breach.[125] The merchant brought suit as assignee and subrogee of its acquiring banks against Visa, alleging various state law claims, including claims that the assessments constitute penalties in violation of unfair competition law.[126] In *Schnuck Markets, Inc. v. First Data Merchant Services Corp*,[127] a grocery store chain brought suit against its acquirer/processer after being subjected to card-network assessments following a data breach, contending the applicable merchant agreement

[120] *Id*. at 6.

[121] Robin Sidel, *Target to Settle Claims Over Data Breach*, WALL ST. J., Aug. 18, 2015, http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013 (last visited Aug. 19, 2015).

[122] *Id.*

[123] No. 3:13cv202, 2013 U.S. Dist. LEXIS 101503 (July 18, 2013 M.D. Tenn.).

[124] *Id.* at *10-15.

[125] *Id.* at 15-16; *see also* Genesco, Inc. v. VISA U.S.A., Inc., 296 F.R.D. 559 (M.D. Tenn. 2014) (ruling on related discovery disputes).

[126] *Genesco, Inc.*, No. 3:13 cv 202, 2013 U.S. Dist. LEXIS 101503, at *42-67.

[127] No. 4:13-CV-2226, 2015 U.S. Dist. LEXIS 4856 (E.D. Mo. Jan. 15, 2015).

contained a $500,000 limitation of liability provision.[128] The court agreed, finding that its two exceptions, for (1) PCI DSS noncompliance with a $3 million limit and (2) "third party fees" and "fees, fines, and penalties" with no limit, did not apply because the assessments were not "fees, fines, and penalties" and that the PCI DSS limit applied to "fines."[129]

[128] *Id.* at *1-4.

[129] *Id.* at *24-29; Schnuck Markets, Inc. v. First Data Merchant Services Corp., No. 4:13-CV-2226, 2015 U.S. Dist. LEXIS 100187, at *7-8 (E.D. Mo. July 31, 2015). In an insurance coverage case, an acquirer bank was subjected to counterfeit fraud and operating expense assessments for a data breach at a card processing firm (which the bank apparently could not pass to the responsible processing firm). First Bank of Delaware, Inc. v. Fidelity and Deposit Co., No. N11C-08-221, 2013 Del. Super. LEXIS 465 (Del. Super. Ct. Oct. 30, 2013). In finding coverage for the insured bank, remarkably the court ruled that coverage effectively extended to the processor's computers, thereby extending the insurer's potential exposure beyond the insured to every processor for which it provided card network access:

> The Court finds that [Data Access System's ("DAS")] computers were used to transact business on behalf of First Bank. DAS's computers were used to conduct card transactions. Part of First Bank's business is earning fees through card transactions. When a card transaction is processed through a member bank's BIN [bank identification number], the member receives a fee. First Bank earned a portion of its non-interest income from the fees associated with its membership in the Visa and MasterCard networks. In First Bank's relationship with DAS, DAS's computer system and First Bank's BIN were both required for either party to benefit from the card transactions. The Court finds that DAS's computer system performing card transactions with First Bank's BIN qualifies as transacting business on behalf of First Bank. *Id.* at *14-15.

Another controversial coverage case involved a merchant's losses following a data breach, including "charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard," the amount of which was determined by settlement between the merchant and its acquirer/processor. Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821, 824-25 (6th Cir. 2012). There, the court found coverage for the merchant's data breach losses under a computer and funds transfer insuring agreement in a blanket crime policy. *Id.* at 826-32. For a discussion of pertinent coverage issues, *see* Toni Scott Reed, *Cybercrime: Losses, Claims, and Potential Insurance Coverage for the Technology Hazards of the Twenty-First Century*, XX FID. L.J. 55 (2014) and Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis*

D. FTC Regulatory Enforcement

Businesses that collect and store consumer information for commercial purposes must comply with an array of federal and state laws. For example, the Gramm Leach Bliley Act of 1999 and accompanying regulations require banks to protect consumers' personal information.[130] Charged with implementing the GLB Act for non-banks, the Federal Trade Commission has issued regulations requiring companies to develop written information security programs to protect customer information.[131]

The FTC has been active in the data-breach arena, deeming inadequate data security practices to constitute unfair or deceptive business practices. Since 2002 the FTC has brought over 50 enforcement actions relating to data security.[132] In 2012, for example, the FTC filed a complaint against Wyndham Hotels for data-security failures that led to three data breaches in less than two years, resulting in the theft of more than 600,000 payment cards and $10.6 million in fraud loss.[133] Wyndham filed a motion to dismiss, challenging the FTC's authority to assert an unfairness claim in the data-security context and contending the FTC needed to formally promulgate regulations before taking action under fair notice principles.[134] The district court denied Wyndham's motion,[135] and on interlocutory appeal, the Third Circuit recently affirmed.[136]

---

of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges, 33 QUINNIPIAC L. REV. 369 (2015).

[130] 15 U.S.C. §§ 6801-6809.

[131] 16 C.F.R. § 314.3(a).

[132] FTC, *Privacy & Data Security Update* (2014), https://www.ftc.gov/reports/privacy-data-security-update-2014#enforcement (last visited Aug. 18, 2015); FTC, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014), *available* at https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf (last visited Aug. 18, 2015).

[133] No. 2:13CV01887, First Am. Compl., FTC v. Wyndham Worldwide Corp. (S.D. Ariz. Aug. 9, 2012), at ¶¶25-40.

[134] FTC v. Wyndham Worldwide Corp., 10 F. Supp. 3d 602, 607 (D.N.J. 2014).

[135] *Id*. at 631.

[136] FTC v. Wyndham Worldwide Corp., No. 14-3514, 2015 U.S. App. LEXIS 14839 (Aug. 24, 2015).

VII.
EMERGING PAYMENT TECHNOLOGIES AND THEIR IMPACT ON PAYMENT CARD FRAUD

A. EMV Chip Card Technology

EMV chip technology in payment cards is currently being implemented in the United States, following Europe's adoption of the technology more than a decade ago. EMV refers to the three founding organizations that developed the chip-based technology: Europay, MasterCard and Visa.[137] Presently, "EMV encompasses specifications, test procedures, and compliance processes managed by EMVCo, LLC, an organisation jointly owned and operated by American Express, Discover, JCB, MasterCard, UnionPay and Visa."[138] EMV in the payment card industry "refers to payment chip cards that contain an embedded microprocessor, a type of small computer that provides strong security features and other capabilities not possible with traditional magnetic stripe cards."[139]

With traditional payment cards using "magnetic stripe technology, the authentication is static. The primary account number, the expiration date, and the cardholder verification value on the magnetic stripe are the same for each transaction."[140] In contrast, payment cards enabled with chip technology use dynamic authentication codes that change with every transaction. Chip card transactions must connect to a chip reader terminal, either via a contact point-of-sale device or ATM or via a contactless terminal with the chip coming within close proximity of the reader.[141] Because the codes change with every transaction, the information being transmitted is of little value to thieves because the information cannot be used for another transaction, nor can the

---

[137] *See* EMVCO, *About EMV*, http://www.emvco.com/about_emv.aspx (last visited Aug. 14, 2015).

[138] *Id.*

[139] *Id.*

[140] Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 3, 26.

[141] EMVCO, LLC, A GUIDE TO EMV CHIP TECHNOLOGY 5-6 (Nov. 2014), *available at* https://www.emvco.com/best_practices.aspx?id=217 (last visited Aug. 26, 2015).

information be used to manufacture a counterfeit card. In other word, chip technology devalues the data from such payment card transactions.[142]

Cards with chip technology may be used with a signature, or may also be equipped for use with a personal identification number, the latter providing for two-factor authentication: the card plus something not on the card; that is, a PIN the cardholder knows. Thus, chip card transactions may be either chip-and-signature or chip-and-PIN. MasterCard and Visa are creating cards that will work as either chip-and-signature or chip-and-PIN, but the issuing banks will determine which configuration is used when the EMV cards are issued.[143]

The adoption of EMV by issuers and merchants, in terms of issuing EMV chip-enabled cards and installing EMV point-of-sale terminals, is a costly endeavor, which is one reason for the delayed introduction here. In the United States, implementation costs are estimated be $9-$10 billion.[144]

To facilitate the adoption of EMV in the United States, the card networks have revised their loss allocation rules to create a "liability shift" for parties that are not EMV-compliant. The first "liability shift" under the rules of the card networks in the United States takes place on October 1, 2015. The liability shifts for fraudulent payment transactions from the issuer to the acquirer/merchant in two general scenarios: (1) when a counterfeit magnetic stripe card with track data copied from a chip card is used at a terminal (for example, card-present) that is not enabled for chip cards; and (2) when a lost or stolen chip-and-PIN card is processed as (i) a magnetic stripe transaction or (ii) a signature chip-card

---

[142] MacCarthy, *supra* note 140, at 26-27.

[143] Sarah Halzack, *Your New Credit Card May Not Be As Safe As You Think*, WASH. POST, Apr. 30, 2015, http://www.washingtonpost.com/news/get-there/wp/2015/04/30/your-new-credit-card-may-not-be-as-safe-as-you-think/ (last visited Aug. 14, 2015). American Express is currently using chip and signature but not chip-and-PIN cards in the United States. *Id.*

[144] Robert Harrow, *Credit Card Fraud: Why EMV Matters in the U.S.*, HUFFINGTON POST, Aug. 5, 2015, http://www.huffingtonpost.com/robert-harrow/credit-card-fraud-why-emv_b_7929310.html (last visited Aug. 14, 2015); MacCarthy, *supra* note 140, at 28.

transaction because the terminal does not support chip-and-PIN.[145] In October 2017, the liability shift will also extend to ATMs and gas station/automated fuel dispensers.[146]

After EMV was adopted in Europe, payment card fraud for card-present transactions declined significantly, and similar results are anticipated in the United States. According to one estimate, "[i]f the use of EMV payment cards in the United States leads to a fraud loss pattern similar to the patterns seen in France, the Netherlands, and the UK, then U.S. fraud losses could fall by as much as 40 percent."[147] One major caveat is that other countries mainly use chip-and-PIN for EMV authentication while issuers in the United States appear likely to use signature verification for EMV transactions rather than PINs. Consequently, "fraud on lost or stolen cards may not decline in the United States."[148]

While fraud for card-present transactions is anticipated to decline from the adoption of EMV cards, other types of payment card fraud are expected to increase. First, issuers and merchants that are late in rolling out EMV cards and terminals and continue to rely on magnetic stripe card technology, may experience an increase in fraud as thieves concentrate on the late-adopters of EMV technology as an easy target.[149] Second, the move to EMV cards will likely result in an increase in card-not-present payment fraud, as online and telephone transactions will remain an attractive outlet for fraudsters.[150] In France, following the adoption of EMV, CNP transactions become the top source of payment

---

[145] EMV MIGRATION FORUM, UNDERSTANDING THE 2015 U.S. FRAUD LIABILITY SHIFTS 2-5 (May 2015), *available at* http://www.emv-connection.com/understanding-the-2015-u-s-fraud-liability-shifts/ (last visited Aug. 31, 2015); VISA, *supra* note 43, at CR-88.

[146] VISA, *supra* note 43, at CR-88.

[147] Richard J. Sullivan, *The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud*, FED. RES. BANK. OF KANSAS CITY ECON. REV., 1Q2013, at 74.

[148] *Id.*

[149] *See id.* at 71-72, 75.

[150] *Id.* at 75; Josephine Wolff, Passing the Buck, Slate, Aug. 4, 2015, *available at* http://www.slate.com/articles/technology/future_tense/2015/08/chip_and_pin_debit_and_credit_cards_won_t_stop_fraud.html (last visited Aug. 11, 2015).

card fraud, accounting for 61 percent of the total value of such fraud in France.[151] Similarly, fraud for CNP transactions grew rapidly in the UK after EMV card implementation, from $333 million in 2005 to $602 million in 2008.[152] Third, fraudsters will likely increase their focus on identity theft as a means of acquiring EMV cards. France, for example, experienced a spike in the incidence of identity theft after the implementation of chip-and-PIN EMV cards.[153]

B. Near Field Communication/Apple Pay

Near Field Communication[154] is a wireless communication technology for mobile payments. A smart chip is incorporated into a NFC-enabled mobile phone into which a payment card and/or other account information is stored. A NFC-enabled mobile phone with a payment card may then be used as a contactless payment device at a contactless point-of-sale reader.[155]

Apple Pay, Samsung Pay, and Android Pay are examples of NFC payment systems.[156] Apple Pay, first announced in September 2014, is available on Apple's iPhone 6, iPad, and Apple Watch.[157] Apple Pay works with all major credit cards and is accepted at 700,000 retail

---

[151] Sullivan, *The U.S. Adoption of Computer-Chip Payment Cards*, *supra* note 147, at 70.

[152] *Id.* at 72.

[153] Christopher Versace, *More Than "Chip-and-Pin" is Needed to Fund Off Card Fraud*, FORBES, May 13, 2015, http://www.forbes.com/sites/ chrisversace/2015/05/13/more-than-chip-and-pin-is-needed-to-fend-off-card-fraud/ (last visited Aug. 31, 2015).

[154] Hereinafter NFC.

[155] BD. OF GOVERNORS OF THE FED. RESERVE SYS., CONSUMER AND MOBILE FINANCIAL SERVICES 2015 13, n.6 (Mar. 2014), *available at* http://www.federalreserve.gov/econresdata/consumerresearch_publications.htm (last visited Aug. 31, 2015); AMERICAN EXPRESS COMPANY, *American Express Mobile NFC Payments*, https://network.americanexpress.com/en/globalnetwork/mobile-nfc/ (last visited Aug. 31, 2015) .

[156] Brad Moon, *Apple Pay vs. Google Pay vs. Samsung Pay: The Digital Wallet War*, INVESTOR PLACE, Jun. 12, 2015, http://investorplace.com/2015/06/apple-samsung-google-android-pay-digital-wallet/ (last visited Aug. 14, 2015).

[157] *Id.*

locations.[158] Samsung Pay, debuted in summer 2015, works with Samsung's new Galaxy phone and via LoopPay, a mobile wallet service.[159] Android Pay, expected to launch in late 2015, is Google's NFC payment system for Android-based mobile devices.[160]

With Apple Pay, a user loads a payment card that is compatible with Apple Pay into the NFC-enabled mobile device. The payment card information is encrypted and assigned a unique device account number that is stored in a dedicated chip in the mobile device.[161] The user activates the touch ID, a biometric fingerprint pad on the mobile device, or enters a passcode, to authorize use. Transactions are then made through tokenization, as further discussed below. When the mobile device is placed in close proximity of the payment terminal, the device account number interacts with the card issuer, which generates a one-time token to process the transaction. With tokenization, the payment card number is not transmitted to the merchant.[162]

Because payment card numbers are not involved in the payment transaction with tokenization, Apple Pay is considered to be a more secure payment method than using a payment card. With Apple Pay, payment card numbers are not accepted, stored, and transmitted by merchants, acquirers, and issuers. Therefore, the payment card data is not at risk of being subjected to theft via a data breach.[163]

To date, the effectiveness of Apple Pay in reducing fraud may be limited for two reasons. First, the onboarding of new cards into NFC-enabled devices proved to be a major vulnerability for Apple Pay. During

---

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] APPLE INC., *Apple Pay, Your Wallet. Without the Wallet*, http://www.apple.com/iphone-6/apple-pay/ (last visited Aug. 14, 2015).

[162] *Id.*; Natalie Gagliordi, *Apple Pay and Security: Could Tokenization be the Tool that Curbs Data Breaches?*, ZDNET, Sept. 11, 2014, http://www.zdnet.com/article/apple-pay-and-security-could-tokenization-be-the-tool-that-curbs-data-breaches/ (last visited Aug. 14, 2015); Avivah Litan, *Will Apple Pay Save Merchants from Data Breaches?*, GARTNER BLOG NETWORK, Sept. 9, 2014, http://blogs.gartner.com/avivah-litan/2014/09/09/will-apple-pay-save-merchants-from-data-breaches/ (last visited Aug. 14, 2015).

[163] *Id.*

the "provisioning" process, thieves were able to load stolen payment card numbers onto iPhones, and then use those devices to make fraudulent transactions via Apple Pay.[164] Each card issuer follows its own provisioning procedures, in which it "performs the customer identification and verification (ID&V) process and reviews information such as device data, geo-location, IP address, and address verification prior to loading the token associated with a consumer's card into the mobile phone."[165] As noted security expert Brian Krebs observed: "The irony here is that while Apple Pay has been touted as a more secure alternative to paying with a credit card, the way Apple and the banks have implemented it actually makes card fraud cheaper and easier for fraudsters."[166] In response to these early problems with provisioning, card issuers implemented additional controls to prevent fraud, such as added controls in call centers, out-of-band verification, and requiring visits to branches in some instances, and there have been no further reports of this type of fraud.[167]

Secondly, the utilization of Apple Pay as a payment method is relatively low. While the market for mobile payment is growing from $52 billion in 2014, and predicted to balloon to $142 billion by 2019, mobile payment still represents a small percentage of the total payment

---

[164] Andrew Ross Sorkin, *Pointing Fingers in Apple Pay Fraud*, N.Y. TIMES, Mar. 16, 2015, http://www.nytimes.com/2015/03/17/business/banks-find-fraud-abounds-in-apple-pay.html (last visited Aug. 14, 2015).

[165] Susan Pandy, FED. RES. BANK OF BOSTON, CURRENT PERSPECTIVES ON THE MOBILE WALLET EVOLUTION 5 (July 8, 2015), *available at* http://www.bostonfed.org/bankinfo/payment-strategies/publications/2015/summary-of-mpiw-meeting-april-2015.htm (last visited Aug. 31, 2015).

[166] Brian Krebs, *Apple Pay: Bridging Online and Big Box Fraud*, KREBS ON SECURITY, Mar. 15, 2015, http://krebsonsecurity.com/2015/03/apple-pay-bridging-online-and-big-box-fraud/ (last visited Aug. 14, 2015).

[167] Pandy, *supra* note 165, at 5, 7 & n.18; Marianne Crowe, *et al.*, FED. RES. BANKS OF ATLANTA AND BOSTON, IS PAYMENT TOKENIZATION READY FOR PRIMETIME? 8, 25-28 (Jun. 11, 2015), *available at* https://www.bostonfed.org/bankinfo/payment-strategies/publications/2015/ tokenization-prime-time.htm?wt.source=bfo_nn (last visited Aug. 31, 2015). Because card issuers are generally responsible for counterfeit card losses, as discussed above, and adopt their own provisioning procedures for onboarding of cards for use with Apple Pay, they are exposed for losses resulting from stolen card data being used with Apple Pay. *See id*. at 25-28.

card market.[168] Further, Apple Pay and the other NFC payment systems in their early stages constitute a small portion of mobile payments, mainly because of the limited acceptance by merchants to date.[169] While Apple Pay is in its infancy, merchants, payment processors and financial institutions alike generally view the new payment method favorably, and its use is expected to grow.[170]

C. Tokenization and Encryption

Tokenization and encryption are different methods for protecting payment card numbers and other data. While EMV chip technology is being deployed on a large scale, and NFC with Apple Pay and other mobile payment methods that also utilize tokenization are in their infancy but growing, the widespread use of tokenization and encryption in the payment card system is considered to be further down the road.

With tokenization, a token is randomly generated as a substitute or surrogate value used to replace sensitive information, such as a payment card number, also known as a primary account number.[171] When used in payment card transactions, a token replaces the card number. The token follows the format of the PAN but otherwise has no mathematical relationship to the PAN, and cannot be reversed-engineered to determine the associated PAN.[172] Encryption does not replace the PAN, but instead "uses a specific algorithm derived from the payment credentials to encode the PAN and other data by masking the characters. The PAN is maintained, but requires authorized parties to use a key to decrypt or reverse the masked credentials back to the PAN."[173]

---

[168] Mike Issac and Brian X. Chen, *Google and Apple Adjust Strategies on Mobile Payments*, N.Y. TIMES, May 27, 2015, http://www.nytimes.com/2015/05/28/technology/google-and-apple-adjust-strategies-on-mobile-payments. html ?_r=0 (last visited Aug. 14, 2015).

[169] Nandita Bose, *In 'Year of Apple Pay,' Many Top Retailers Remain Skeptical*, REUTERS, Jun. 5, 2015, http://www.reuters.com/article/2015/06/06/us-apple-pay-idUSKBN0OL0CM 20150606 (last visited Aug. 14, 2015).

[170] Pandy, *supra* note 165, at 12-13; Crowe, *et al.*, *supra* note 167, at 28-31.

[171] Hereinafter PAN.

[172] Crowe, *et al.*, supra note 167, at 8.

[173] *Id.*

Tokenization "eliminates the need for merchants to store the full PAN on their network systems" and reduces "the financial impact resulting from data compromise, theft, or unintended disclosure during disposal."[174] In other words, tokenization devalues the data that is being captured, transmitted, and stored.

As an emerging technology, tokenization models and standards have been developed by multiple participants in the payments industry. Generally there are two models for tokenization: security tokens and payment tokens. Security tokens are used to replace payment card numbers after the payment-authorization process has begun or for stored data, such as in a merchant's database. These token are used to secure and protect data, not to create a token to replace a payment card during a financial transaction.[175]

Payment tokens, a relatively recent development, involve a random value that replaces a payment card number for the payment transaction. Payment tokens may be dynamic, static, or both. Dynamic tokens are valid for a single transaction or limited number of transactions. Static token are those whose value does not change, allowing multi-use and merchants the ability to connect with a cardholder's transaction history. Payment tokens can be combined when a static token is combined with a uniquely generated cryptogram[176] for encrypting the payment transaction.[177]

The optimal utilization of tokenization and encryption may be summarized as follows:

---

[174] Susan Pandy and Marianne Crowe, FED. RES. BANK. OF BOSTON, MOBILE PAYMENTS INDUSTRY WORKGROUP MEETING DISCUSSION ON TOKENIZATION LANDSCAPE IN THE U.S. 3 (Sept. 23, 2014), *available at* https: //www.bostonfed.org/bankinfo/payment-strategies/publications/2014/sum-mary-of-mpiw-meeting-june-2014.htm (last visited Aug. 31, 2015).

[175] Crowe, *et al*., supra note 167, at 5.

[176] "A cryptogram is a transaction security key that supports dynamic authentication or the use of changing variables unique to each individual card transaction. For a mobile transaction, the NFC chip generates the cryptogram in the mobile phone versus a chip on a credit card." *Id*. at 7, n. 17.

[177] *Id*. at 6-7.

> Security tokenization is effective if the PAN is not tokenized when payment is initiated. Even then, security tokenization only protects the PAN post-authorization and at-rest after the transaction process is completed. If the PAN is replaced initially with a payment token, the PAN is eliminated from the transaction flow, and some would argue that this eliminates the need for a security token to be created at all. However, until payment tokenization is ubiquitous, using a multi-layered combination of payment and security tokens, coupled with encryption, will increase the security of payment data. Fundamentally, this is viewed as the best available approach to payment data security for card, digital, and mobile payments (where tokens enhance the security of the near field communication (NFC) chip). Implementing only one solution leaves aspects of the payment system still vulnerable.[178]

Another technology for payment card transactions is 3-D Secure, a "secure communication protocol used to enable real-time cardholder authentication directly from the card issuer during an online transaction . . . ."[179] "3-D" refers to a three-domain model: (1) acquirer/merchant domain; (2) card issuer domain; and (3) interoperability domain used to support the online transaction (such as credit and debit).[180] A cardholder enrolls the card in 3-D Secure by selecting a PIN for 3-D Secure transactions. A merchant must also enroll in 3-D Secure. When a cardholder uses a card enrolled in 3-D Secure at an online merchant participating in 3D Secure, the cardholder is directed to a pop-up window at checkout to enter the 3-D PIN before completing the transaction.[181]

3-D was launched in 2004 as Verified by Visa, MasterCard Secure Code, and American Express SafeKey, but has not been widely used. Although they bear the loss for fraud losses, online merchants have not embraced 3-D Secure for fear of lost sales from shopping cart

---

[178] *Id.* at 8.
[179] *Id.* at 42.
[180] *Id.* at 42-43.
[181] *Id.* at 43.

abandonment by adding another security step.[182] As card issuers and cardholder generally do not bear the loss for card-not-present fraud, they have not been interested in utilizing 3-D Secure.[183] With the anticipated shift in online CNP fraud due to the migration to EMV chip cards, however, the payment card industry has expressed a renewed interest in 3-D Secure, and EMVCo has assumed oversight of 3-D Secure to develop an improved authentication solution, with an anticipated EMV protocol in 2016.[184]

In sum, "tokenization is viewed as a key component for improving the security of retail payments and protecting payment credentials by removing them from the transaction process."[185] As discussed above, Apple Pay has been the leader in using tokenization, making "the use of payment tokenization for retail payments an implementable reality and scalable solution. This concept has provided the industry with a stronger conform level around security by combing NFC with a token and cryptogram stored in the secure element, and optional fingerprint authentication."[186]

VIII.
CONCLUSION

The allocation of losses for payment card fraud is changing. Driven by data breaches and technology, liability for payment card fraud is shifting from card issuers to acquirers and merchants. In effect, the governing principle of the Uniform Commercial Code—the party in the best position to avoid the loss should ultimately bear the loss—is being adapted to the payment card arena.

[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.* at 50.
[186] *Id.* at 50-51.