UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

ARKANSAS FEDERAL CREDIT UNION and THE SUMMIT FEDERAL CREDIT UNION, on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. HUDSON'S BAY COMPANY, SAKS FIFTH AVENUE LLC, SAKS & COMPANY LLC, SAKS INCORPORATED, and LORD & TAYLOR, LLC, Defendants.	Case No. 19-cv-4492 (PKC) **SECOND AMENDED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs Arkansas Federal Credit Union and The Summit Federal Credit Union ("Plaintiffs"), through their undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, file this Class Action Complaint against Defendants Hudson's Bay Company ("HBC"); Saks Fifth Avenue LLC, Saks & Company LLC, and Saks Incorporated, (collectively, "Saks"); and Lord & Taylor, LLC ("Lord & Taylor") (collectively, "Hudson Bay" or "Defendants"). Plaintiffs' allegations are made based on personal knowledge, as to Plaintiffs and Plaintiffs' own acts, and on information and belief and investigation of counsel, as to all other matters.

INTRODUCTION

1. This is a class action on behalf of financial institutions that suffered, and continue to suffer, financial losses as a result of Hudson Bay's conscious decsion to implement inadequate measures to protect Plaintiffs' and other financial institutions' payment card data from being stolen from Hudson Bay's point-of-sale ("POS") and computer systems. From approximately May 1,

2017, to March 31, 2018, Hudson Bay allowed computer hackers, the notorious Fin7 syndicate, to enter Defendants' computer systems undetected and install malware that infected Saks' and Lord & Taylor's POS systems at all Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor locations in North America (the "Data Breach"). The malware enabled the hackers to steal the cardholder names, credit and debit card numbers, card expiration dates, card verification values, service codes, and other information (collectively, "Payment Card Data") from ***more than five million*** payment cards issued by Plaintiffs and the Class (defined below) that were compromised. The stolen Payment Card Data was then offered for sale and sold on the dark web by the hackers and used by cyber-criminals to make fraudulent purchases.

2. This confidential Payment Card Data was compromised because of Hudson Bay's affirmative acts in implementing data security measures that were inadequate to properly protect the Payment Card Data that Plaintiffs and the Class entrusted to Hudson Bay. Hudson Bay, by accepting payment cards at its stores, knew, or should have known, it was required to adequately protect Payment Card Data.

3. The susceptibility of POS systems to malware is well known throughout the retail industry. In the last five years, malware placed on POS systems caused practically every major data breach involving retail stores, resulting in millions of compromised payment cards.

4. Despite the susceptibility of POS systems to hacking, a data breach that compromises sensitive payment card information is not an inevitability of doing business; rather, numerous measures can be taken to prevent intrusion by unauthorized personnel into POS devices and networks and to limit the effect of an intrusion if it occurs. For example, one data security expert recommends a "**Tripod of POS Security**," comprised of the following protective measures: (a) POS systems that support EMV chip-based payment cards (a secure method of transmitting

credit card data that replaces the traditional magnetic stripe); (b) end-to-end encryption, which encrypts Payment Card Data as soon as payment cards are swiped; and (c) tokenization, which replaces credit and debit card numbers with a meaningless series of letters and numbers, rendering any information collected by hackers useless.[1]

5. Another data security expert commented that:

> POS systems are not difficult to secure if merchants would simply follow the advice that has been put out by [industry experts]. Most of the advice is based on security best practices ***that have been around for years***. Unfortunately, it often takes a data breach for companies to have their eyes opened to the impact their negligence can have.[2]

[Emphasis added].

6. Despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable POS systems and inadequately protected computer networks, Hudson Bay took inadequate measures to prevent or detect the Data Breach, as the hackers launched their malicious payloads and ultimately exfiltrated Payment Card Data for over eight months from Hudson Bay's computer network. Hudson Bay knowingly refused to implement certain best practices, ignored explicit warnings about the vulnerability of its POS system, and disregarded and/or violated applicable industry standards. For example, as described herein, Defendants ignored well-known data security risks and intentionally allowed specific data security deficiencies to persist; refused to implement certain security measures that would have protected Payment Card Data; failed to install software to adequately track access to its network,

---

[1] *Point of sale security: Retail data breaches at a glance*, DATACAP SYS., INC. (May 12, 2016), https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#.

[2] John H. Sawyer, *Tech Insight Defending Point-Of-Sale Systems*, DARKREADING (Jan. 24, 2014, 4:53 PM), https://www.darkreading.com/attacks-breaches/tech-insight-defending-point-of-sale-systems/d/d-id/1141214.

monitor the network for unusual activity, and prevent exfiltration of payment card data, which would have detected the presence of the malware installed by the hackers and prevented Payment Card Data from being stolen; and chose not to implement end-to-end encryption technology or tokenization for use with its POS systems, which would have protected Payment Card Data or render the payment card data useless to the hackers.

7. Plaintiffs and the Class have suffered financial losses as a result of the Data Breach. Specifically, Plaintiffs and other financial institutions have been forced to: (a) cancel or reissue any credit and debit cards identified by a payment card network as compromised in the Data Breach; (b) stop payments and block transactions from any deposit, transaction, checking, or other accounts that are linked to debit cards that were identified by a payment card network as compromised in the Data Breach or closing such accounts; (c) refund any cardholder for any unauthorized transaction on payment cards that were identified by a payment card network as compromised in the Data Breach; and (d) respond to a higher volume of cardholder complaints, confusion, and concern.

8. This class action is brought on behalf of financial institutions throughout the United States to recover the damages that they and others similarly situated have suffered, and continue to suffer, as a direct result of the Data Breach. Plaintiffs assert claims for negligence, negligence per se, violation of state consumer protection statutes, unjust enrichment, and declaratory and ancillary equitable relief.

PARTIES

9. Plaintiff Arkansas Federal Credit Union ("Arkansas FCU") is a federally chartered credit union with its principal place of business in Jacksonville, Arkansas, and is a citizen of Arkansas. Plaintiff Arkansas FCU employs numerous methods to maintain the confidentiality of its Payment Card Data and to prevent disclosure of its Payment Card Data to unauthorized third

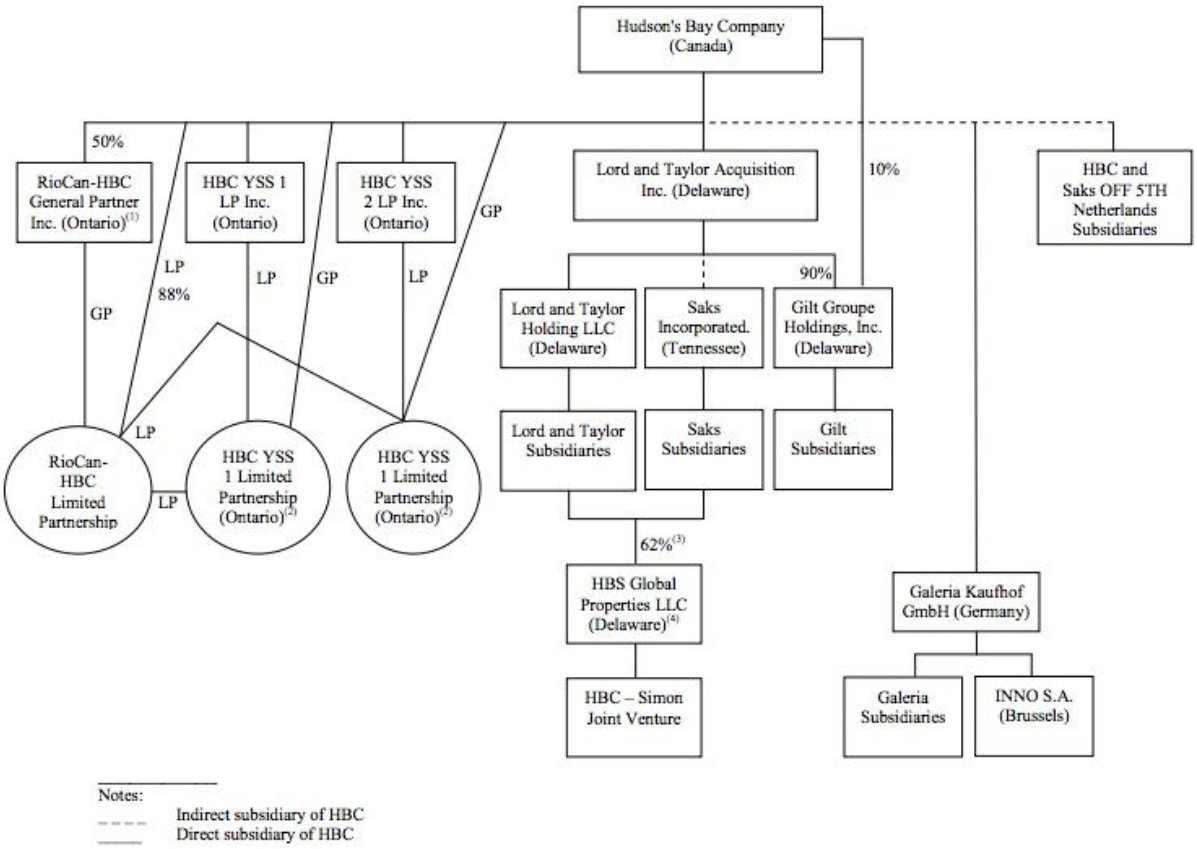
parties. As a result of the Data Breach, Plaintiff Arkansas FCU has incurred direct out-of-pocket costs and suffered, and continues to suffer, injuries, including, *inter alia*, costs associated with: (a) canceling and reissuing payment cards that were identified by a payment card network as compromised in the Data Breach; (b) stopping payments and blocking transactions from deposit, transaction, checking, or other accounts that are linked to debit cards that were identified by a payment card network as compromised in the Data Breach or closing such accounts; (c) fraud losses incurred in the wake of the Data Breach resulting from unauthorized transactions on payment cards that were identified by a payment card network as compromised in the Data Breach; and (d) responding to a higher volume of cardholder complaints, confusion, and concern. Among other things, Plaintiff Arkansas FCU received at least one fraud alert from a payment card network notifying it that payment cards that it issued were used at Hudson Bay and compromised in the Data Breach. As a result of the Data Breach, Plaintiff Arkansas FCU canceled and reissued the payment cards that were identified as compromised in the Data Breach. Plaintiff Arkansas FCU is subject to an imminent threat of future harm because Hudson Bay's response to past data breaches has been so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

10. Plaintiff The Summit Federal Credit Union ("Summit FCU") is a federally chartered credit union with its principal place of business in Rochester, New York, and is a citizen of New York. Plaintiff Summit FCU employs numerous methods to maintain the confidentiality of its Payment Card Data and to prevent disclosure of its Payment Card Data to unauthorized third parties. As a result of the Data Breach, Plaintiff Summit FCU incurred direct out-of-pocket costs and has suffered, and continues to suffer, injuries, including, *inter alia*, costs associated with canceling and reissuing payment cards that were identified by a payment card network as

compromised in the Data Breach. Specifically, Plaintiff Summit FCU received at least one fraud alert from a payment card network notifying it that payment cards that it issued were used at Hudson Bay and compromised in the Data Breach. As a result of the Data Breach, Plaintiff Summit FCU canceled and reissued the payment cards it issued that were compromised in the Data Breach, which included payment cards that were issued to members who are citizens of New York. Plaintiff Summit FCU is subject to an imminent threat of future harm because Hudson Bay's response to past data breaches has been so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

11. Defendant HBC is a Canadian corporation with its principal place of business in New York, New York. As of February 2018, HBC operated 50 Lord & Taylor stores, 41 Saks Fifth Avenue stores, and 129 Saks OFF 5TH stores.[3] HBC is the ultimate parent company for each of the other Defendants and owns Saks and Lord & Taylor stores. HBC's corporate structure is represented as follows:

[3] *HBC 2017 Annual Report* at 14, HUDSON'S BAY CO. (Feb. 3, 2018), http://investor.hbc.com/static-files/5c6545ac-37f0-4b52-a6b2-1d54ab3c7b6f.



In 2018, Hudson Bay's revenues totaled approximately $14.3 billion.

12. Defendant Saks Fifth Avenue LLC is a Massachusetts limited liability company with its principal place of business in New York, New York. The sole member of Saks Fifth Avenue LLC is Saks & Company LLC.

13. Defendant Saks & Company LLC is a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Saks & Company LLC is Saks Incorporated.

14. Defendant Saks Incorporated is a Tennessee corporation with its principal place of business in New York, New York.

15. Defendant Lord & Taylor is a Delaware limited liability company with its principal place of business in New York, New York. The sole member of Defendnat Lord & Taylor is Lord & Taylor Holdings LLC, a Delaware limited liability company, with its principal place of business in New York, New York. The sole member of Lord & Taylor Holdings LLC is Lord & Taylor Acquisition Inc., a Delaware corporation.

JURISDICTION AND VENUE

16. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. §1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, many of which are citizens of a different state than Defendants. Defendant HBC is a citizen of Canada, where it is incorporated, Defendant Saks is a citizen of Tenessee, where it is incorporated, and Defendant Lord & Taylor is a citizen of Delaware, where it is incorporated. The Court also has subject matter jurisdiction over Plaintiffs and the proposed Class's claims pursuant to 28 U.S.C. §1367(a).

17. The Southern District of New York has personal jurisdiction over Defendants because Defendants conduct substantial business in this District and maintain their principal places of business in this District.

18. Venue is proper in this Court, pursuant to 28 U.S.C. §1391, because Defendants reside in this District, regularly transact business in this District, and a substantial part of the events giving rise to this action arose in this District.

FACTUAL BACKGROUND

A. Hudson Bay Had a Duty to Protect Payment Card Data in Light of the Foreseeability of the Risk It Created by Knowingly Implementing Inadequate Data Security Measures

19. Plaintiffs and the Class are financial institutions that issue payment cards, such as credit and debit cards, to their customers.

20. Hudson Bay stores accept payment cards for the purchase of goods. A substantial portion of Hudson Bay's sales are attributable to credit and debit card transactions. In processing payment card transactions through its POS system, Hudson Bay acquires a substantial amount of Payment Card Data.

21. A POS system is an on-site device that manages both cash and payment card transactions from consumer purchases. When a payment card is used at a POS terminal, "data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."[4] Before transmitting customer data over the merchant's network, POS systems typically, and very briefly, store the data in plain text within the system's memory. *Id.* at 5. Likewise when an EMV chip card is used at a POS terminal, '"[i]nstead of going to a register and swiping your card, you are going to do what is called "card dipping" instead, which means inserting your card into a terminal slot and waiting for it to process[.]"'[5] Additionally, like with a magnetic stripe card, '"[w]hen an EMV card is dipped, data flows between the card chip and the issuing financial institution to verify the card's legitimacy and

---

[4] *SECURITY RESPONSE: A Special Report on Attacks on point-of-sales systems* at 6, SYMANTEC CORP. (Nov. 20, 2014), https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf.

[5] Sienna Kossman, *8 FAQs about EMV credit cards*, CREDITCARDS.COM (Aug. 29, 2017), https://www.creditcards.com/credit-card-news/emv-faq-chip-cards-answers-1264.php.

create the unique transaction data." *Id.* According to First Data Corporation ("First Data"), a leading payment processor: "[c]urrently, in the majority of both EMV and non-EMV transactions, payment card information is sent from the point-of-capture to the acquirer/processor 'in the clear,' i.e., in an unencrypted form."[6] Any time that Payment Card Data is "in the clear" – that is, in plain text format that is readable by a person or computer – it is extremely vulnerable to theft. It is this unencrypted Payment Card Data on the POS system that hackers seek to access.

22. It is well known that Payment Card Data has considerable value to and often is targeted by hackers, who easily can sell Payment Card Data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[7] Tim Erlin, Vice President of Tripwire, a threat, security, and compliance solutions vendor, noted that "'[a]s long as compromised credit card data continues to be a valuable commodity on the black market, any company collecting or processing valid credit card information will continue to be a high value target[.]'"[8] Intruders with access to Payment Card Data can physically replicate the card or use it online. Unsurprisingly, theft of payment card information via POS systems is now "one of the biggest sources of stolen payment cards."[9]

---

6 *EMV and Encryption + Tokenization: A Layered Approach to Security* at 5, FIRST DATA CORP. (2012), https://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF.

7 Brian Krebs, *The Value of a Hacked Company*, KREBS ON SEC. (July 14, 2016, 10:47 AM), https://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

8 Dan Rayward, *Chipotle Reports Suspicious Activity on POS System*, INFOSEC. MAG. (Apr. 26, 2017), https://www.infosecurity-magazine.com/news/chipotle-suspicious-activity-pos/.

9 A Special Report on Attacks at 3, *supra* n.4.

23. Over the last several years, numerous data breaches have occurred at large retailers nationwide, including Target, Home Depot, Eddie Bauer, Sally Beauty, Harbor Freight Tools, and Kmart, among many others.

24. Each of these massive data breaches involved malware placed on each merchant's POS system. For example, in 2013, hackers infiltrated Target's POS system, stealing information from an estimated 40 million payment cards in the United States.[10] In 2014, over 7,500 self-checkout POS terminals at Home Depot locations throughout the United States were hacked, compromising roughly 56 million debit and credit cards. *Id.* at 4, 7. In 2016, on-site POS systems at more than 1,000 Wendy's restaurants were infiltrated with malware, resulting in the theft of Payment Card Data for nearly six months.[11]

25. Despite the well-known vulnerabilities of POS systems, available security measures and business practices would have significantly reduced or eliminated hackers' ability to successfully infiltrate merchants' POS systems. One report indicated that over 90% of the data breaches occurring in 2017 were preventable.[12]

26. Certain data security organizations, federal agencies, and state governments have implemented recommended standards of care regarding security measures designed to prevent these types of intrusions into POS systems. Hudson Bay's adherence to reasonable standards of care could have either prevented or timely detected this Data Breach.

---

[10] Brett Hawkins, *Case Study: The Home Depot Data Breach* at 3-4, SANS INSTIT. (Jan. 2015), https://www.sans.org/reading-room/whitepapers/casestudies/casestudy-home-depot-data-breach-36367.

[11] Brian Krebs, *1,025 Wendy's Locations Hit in Card Breach*, KREBS ON SEC. (July 8, 2016), https://krebsonsecurity.com/2016/07/1025-wendys-locations-hit-in-card-breach/.

[12] *Cyber Incident & Breach Trends Report* at 3, ONLINE TR. ALL. (Jan. 25, 2018), https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.

27. Hudson Bay is, and at all relevant times was, aware that the Payment Card Data it receives and maintains is confidential and highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

28. Hudson Bay is, and at all relevant times was, fully aware of the significant volume of daily payment card transactions at Hudson Bay's stores, amounting to tens of thousands of daily payment card transactions, and thus, the significant number of payment cards that would be impacted by a breach of Hudson Bay's POS systems.

29. Hudson Bay is, and at all relevant times has been, aware of the importance of safeguarding Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, including the significant harm that Plaintiffs and the Class would suffer. Indeed, in a press release relating to the Data Breach, Hudson Bay advised consumers to "review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize."[13]

30. Despite Hudson Bay's understanding of the risk it created in leaving its POS systems vulnerable to a malware attack, Hudson Bay took unreasonable and insufficient measures to protect Payment Card Data by choosing not to employ widely available resources to prevent or detect an intrusion.

B. The Hudson Bay Data Breach

31. For over eight months – from approximately May 1, 2017, to March 31, 2018 – malware existed undetected on POS systems at Saks Fifth Avenue, Saks OFF 5TH, and Lord &

[13] Press Release, Hudson's Bay Co., HBC Provides Information about Data Security Issue in Certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor Stores in North America (Apr. 1, 2018), http://investor.hbc.com/news-releases/news-release-details/hbc-provides-information-about-data-security-issue-certain-saks.

Taylor locations. The malware installed on Hudson Bay's POS systems allowed hackers to access and exfiltrate both Track 1 and Track 2 data. Track 1 Payment Card Data refers to a cardholder's name, primary account number, expiration date, card verification value/code, and service code; and Track 2 Payment Card Data refers to primary account number, expiration date, card verification value/code, and service code.

32. On March 28, 2018, hackers identifying themselves as "JokerStash" (also known as "Fin7") announced, in part, via the following image, the release of a compromised batch of Payment Card Data that the hackers referred to as "BIGBADABOOM-2."[14]

33. On April 1, 2018, the cyber threat consulting firm Gemini Advisory ("Gemini") announced that, working with "several financial organizations," it had "confirmed with a high degree of confidence that the compromised records" referenced in the JokerStash announcement

[14] *Fin7 Syndicate Hacks Saks Fifth Avenue and Lord & Taylor Stores*, GEMINI ADVISORY (Apr. 1, 2018), https://geminiadvisory.io/fin7-syndicate-hacks-saks-fifth-avenue-and-lord-taylor/.

"were stolen from customers of Saks Fifth Avenue and Lord & Taylor stores." *Id.* Gemini noted that the hackers associated with JokerStash had been involved with other well-publicized data breaches, including those at Whole Foods, Chipotle, Omni Hotels & Resorts, and Trump Hotels, some of which involved compromised POS systems. *Id.*

34. According to Gemini's analysis, the compromise at Hudson Bay began in May 2017. *Id.* Gemini reported that the hackers claimed to have compromised ***more than five million payment cards***. *Id.* By Gemini's accounts, as of April 2018, hackers were already offering for sale compromised Payment Card Data associated with 35,000 records from Saks and 90,000 records from Lord & Taylor. *Id.*

35. Gemini further stated that given that customers who "frequently shop at luxury retail chains like Saks Fifth Avenue are more likely to purchase high-ticket items regularly[,]" it would thus "be extremely difficult to distinguish fraudulent transactions from those of a legitimate nature, allowing criminals to abuse stolen payment cards and remain undetected for a longer period of time." *Id.* To defray this risk, Gemini recommended that payment cards be replaced. *Id.*

36. Following publication of Gemini's announcement, on April 1, 2018, Hudson Bay issued a press release confirming the Data Breach:

> HBC (TSX:HBC) today announced that it has become aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. While the investigation is ongoing, there is no indication at this time that this affects the Company's e-commerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe.
>
> The Company deeply regrets any inconvenience or concern this may cause. HBC wanted to reach out to customers quickly to assure them that they will not be liable for fraudulent charges that may result from this matter. HBC has identified the issue, and has taken steps to contain it. Once the Company has more clarity around the facts, it will notify customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. HBC encourages customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.

> The Company is working rapidly with leading data security investigators to get customers the information they need, and the investigation is ongoing. HBC is also coordinating with law enforcement authorities and the payment card companies.
>
> For further information, please visit https://www.saksfifthavenue.com/security-information/notice.html,https://www.saksoff5th.com/security-information/notice.html, or https://www.lordandtaylor.com/security-information/notice.html.
>
> In the coming days, customer care representatives will be available through a dedicated call center to provide further information. The call center information will be posted on the above websites at that time.[15]

37. On April 27, 2018, Hudson Bay issued a second press release providing an update regarding the Data Breach:

> HBC (TSX:HBC) today provided an update on its investigation into the previously-disclosed data security issue involving customer payment card data at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America.
>
> HBC contained the issue on March 31, 2018 and believes it no longer poses a risk to customers shopping at its stores. ***The company wants to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter***.[16]

[Emphasis added].

38. On April 11, 2018, Visa issued the first of a series of Compromised Account Management System ("CAMS") alerts regarding the Data Breach to financial institutions. In an April 20, 2018, follow-up CAMS alert, Visa identified that the the estimated fraud "exposure window" for the Data Breach ran from May 1, 2017, through March 31, 2018. The CAMS alert further indicated that both Track 1 and Track 2 Payment Card Data was compromised in the Data Breach. On September 13, 2018, Visa further indicated that there had been a "confirmed network

---

15 HBC Provides Information about Data Security Issue, *supra* n.13.

16 Press Release, Hudson's Bay Co., HBC Provides Update on Previously-Announced Data Security Issue at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor Locations in North America (Apr. 27, 2018), http://investor.hbc.com/news-releases/news-release-details/hbc-provides-update-previously-announced-data-security-issue.

intrusion" associated with the Data Breach, and that the "confirmed unauthorized access . . . included full track two data," including the compromise of Payment Card Data such as account numbers, expiration dates, and cardholders' names.

39. Hudson Bay's data security systems suffered from many deficiencies that made them susceptible to hackers. Hudson Bay knowingly:

(a) ignored well-known data security risks, thereby intentionally allowing data security deficiencies to persist;

(b) refused to implement certain security measures that would have protected Payment Card Data;

(c) failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of the hackers and prevented Payment Card Data from being stolen; and

(d) chose not to implement end-to-end encryption technology or tokenization for use with its POS systems, which would have protected Payment Card Data and rendered it useless to the hackers.

C. Hudson Bay Breached Its Duty to Avoid Causing Plaintiffs and the Class Foreseeable Harm by Consciously Disregarding Known Risks

1. Despite Well-Known Risks, Hudson Bay's Lackadaisical Approach to Data Security Allowed Deficiencies to Persist

40. Much of the blame for the state of Hudson Bay's data security systems can be placed squarely with Hudson Bay's senior management, who knew, or should have known, that its data security efforts were deficient given numerous well-publicized threats, including those aimed at Hudson Bay. Yet, Hudson Bay did not prioritize data security or devote adequate resources to address security issues, thereby allowing data security deficiencies to persist.

41. Hudson Bay knew, or should have known, of the threat of a data breach given the prior high-profile breaches that occurred at Target, Home Depot, Wendy's, Arby's, Eddie Bauer, and others and that payment cards brands and others routinely notified merchants of the cybersecurity threats that were specifically targeting the retail and restaurant sectors. As early as October 2008, Visa issued a "Data Security Alert" describing the threat of RAM scraping malware.[17] In May 2009, Visa issued an updated Data Security Alert warning merchants that due to a memory parsing (RAM scraping) vulnerability "hackers are gaining unauthorized access to point-of-sale (POS) environments as a result of insecure remote desktop solutions or poor network configuration."[18] The May 2009 alert instructs companies to "secure their external and internal network perimeters to prevent unauthorized access to POS systems, payment processing servers, database servers or other servers where payment card data resides." *Id*. The May 2009 alert further instructs merchants to: "Secure your remote access connectivity"; "Implement a secure network configuration including egress and ingress filtering to only allow the ports/services necessary to conduct business" (*i.e.*, segregate networks); "Monitor firewalls for suspicious traffic (particularly outbound traffic to unknown addresses)"; "Implement file integrity monitoring"; "Secure systems so that unauthorized software cannot be installed"; "Ensure that all anti-virus and anti-spyware software programs are up-to-date"; and "Routinely examine systems and networks for newly-added hardware devices; unknown files and software." *Id*.

---

[17] Numaan Huq, *2014 - An Explosion of Data Breaches and PoS RAM Scrapers*, TREND MICRO: TREND LABS SEC. INTELLIGENCE BLOG (Sept. 11, 2014, 2:16 AM), http://blog.trendmicro.com/trendlabs-security-intelligence/2014-an-explosion-of-data-breaches-and-pos-ram-scrapers/.

[18] Visa Data Security Alert, *Targeted Hospitality Sector Vulnerabilities*, FIRST DATA CORP. (May 28, 2009), https://webcache.googleusercontent.com/search?q=cache:inr6SWDrgc8J:https://www.firstdata.com/downloads/partners/fd_gpm_notice_visa_security_alert_28may09_partnersupport.doc+&cd=8&hl=en&ct=clnk&gl=us.

42. Indeed, in August 2013, Visa warned merchants of malware targeting POS systems. Specifically, the alert, entitled "Retail Merchants Targeted by Memory-Parsing Malware," warned: "Since January 2013, Visa has seen an increase in network intrusions involving retail merchants. Once inside the merchant's network, the hacker will install memory parser malware on the Windows based cash register system in each lane."[19]

43. In February 2014, Visa again warned merchants of the increased risks posed by malware designed to target POS systems in an update to its August 2013 security alert. Specifically, the February 2014 alert stated:

> Visa is issuing this alert to make clients aware of new malware information and to remind Visa merchants to secure their payment processing (and non-payment) networks from unauthorized access. Visa highly recommends merchants implement these signatures on security solutions to detect a suspected breach. However, Visa recommends performing sufficient due diligence prior to implementing any block to avoid any inadvertent connectivity issues for legitimate access.[20]

44. U.S. Computer Emergency Readiness Team ("U.S. CERT"), a government unit within the Department of Homeland Security, also alerted retailers to the threat of POS malware in two separate alerts, on January 2 and July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware.[21]

---

[19] Visa Data Security Alert, *Retail Merchants Targeted by Memory-Parsing Malware – UPDATE*, VISA (Aug. 2013), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin__Memory_Parser_Update_082013.pdf.

[20] Visa Data Security Alert, *Retail Merchants Targeted by Memory-Parsing Malware – UPDATE*, VISA (Feb. 2014), https://usa.visa.com/dam/VCOM/download/merchants/Bulletin-Memory-Parser-Update-012014.pdf.

[21] *See Alert (TA14-002A): Malware Targeting Point of Sale Systems*, U.S. DEP'T OF HOMELAND SEC. (Jan. 2, 2014; revised Oct. 6, 2016), https://www.us-cert.gov/ncas/alerts/TA14-002A; *Alert (TA14-212A): Backoff Point-of-Sale Malware*, U.S. DEP'T OF HOMELAND SEC. (July 31, 2014; revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.

45. Hudson Bay knew, or should have known, of the susceptibility of its POS systems and that a breach of its corporate network would permit intruders to install malware at its locations throughout the United States, putting Plaintiffs' and the Class's Payment Card Data at risk.

46. In its April 2017 Annual Information Form, Hudson Bay acknowledged that ***"[a] potential privacy breach could have a material adverse effect on our business and results of operations***."[22] Further, Hudson Bay recognized the specific risk that "an unauthorized party may obtain access to our data systems and misappropriate business and personal information." *Id.*

47. Hudson Bay therefore should have been aware of the need to have adequate data security systems in place.

48. Hudson Bay was also on notice that its data security systems were insufficient given prior data security incidents at the company.

49. In March 2017, it was discovered that personal information for tens of thousands of Saks customers was publicly available on Saks's website.[23] The personal information included Saks customers' email addresses, product codes for the items customers expressed interest in buying, phone numbers, dates and times the customers visited Saks' website, and IP address from which they visited. *Id.*

50. The personal information was unencrypted and stored in plain text on Saks's website for anyone to access. *Id.*

---

22 Hudson Bay Co., *ANNUAL INFORMATION FORM* at 61 (Apr. 28, 2017), http://investor.hbc.com/static-files/c86b36ab-460c-4e7f-98c9-3fd02f924446.

23 Leticia Miranda, *Saks Fifth Avenue Exposed Personal Info On Tens Of Thousands Of Customers*, BUZZFEED NEWS (Mar. 19, 2017, 1:17 PM ET; updated Mar. 20, 2017, 12:49 AM ET), https://www.buzzfeednews.com/article/leticiamiranda/saks-fifth-avenue-exposed-personal-info#.rrRG2Bpqr.

51. Moreover, Saks failed to encrypt visitor traffic to several of its websites, leaving customers' information vulnerable to hackers if customers browsed Saks's website over open Wifi networks. *Id.*

52. Robert Graham ("Graham"), quoted by news outlets as a cybersecurity expert, remarked that Saks's exposure of personal information was '"as bad as security gets'" and that '"[e]veryone [was] vulnerable.'" *Id.* Presciently, Graham also remarked of Saks's security practices, '"[w]here there's smoke, there's fire[.]'" *Id.*

53. At the time, Hudson Bay stated that it took the matter '"seriously,'" and that '"[t]he security of [its] customers is of utmost priority.'" *Id.* Hudson Bay further stated that it was '"moving quickly and aggressively to resolve the situation[.]'" *Id.*

54. Despite acknowledging such risks, Hudson Bay disregarded the potential danger of a data breach by failing to devote adequate resources to address security issues and failing to take adequate steps to implement reasonable data security measures to prevent or timely detect the Data Breach.

55. Indeed, Hudson Bay devoted substantial resources to building out its Saks and Lord & Taylor stores. In April 2016, it announced a "higher-than-normal capital budget" of up to $850 million.[24] Of that, 30% was devoted to "expanding the retail portfolio of its Saks Fifth Avenue division with seven new full-line Saks stores and 32 new Saks Off 5th off-price stores." *Id.* Another 40% was devoted to "store rennovations," and the remaining 30% was devoted to miscellaneous "technology investments, such as the robotic automation of the company's

[24] Mike Troy, *Surging Hudson's Bay details major investments in expanding Saks, Saks Off 5th and store renovations*, CHAIN STORE AGE (Apr. 5, 2016), https://www.chainstoreage.com/news/surging-hudsons-bay-details-major-investments-expanding-saks-saks-th-and-store-renovations/.

distribution center in Toronto and a new e-commerce fulfillment center in the U.S." *Id.* Despite this nearly billion-dollar investment, Hudson Bay did not, apparently, choose to invest in data security issues or provide the resources necessary to implement reasonable data security measures to protect Plaintiffs' and the Class's Payment Card Data.

2. Hudson Bay Refused to Implement Protocols that Would Have Protected Payment Card Data

56. Hudson Bay knowingly failed to implement certain protocols that would have protected Plaintiffs' Payment Card Data in the event of a data breach.

57. Payment Card Data for a purchase transaction must flow through multiple systems and parties in order to be processed. For most merchants, there are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen because it exists "in the clear":

(a) Pre-authorization: When the merchant has captured the Payment Card Data and it is being sent or is waiting to be sent to the acquirer/processor; and

(b) Post-authorization: When Payment Card Data has been sent back to the merchant with the authorization response from the acquirer/processor, and it is placed into some form of storage in the merchant environment and used for analytics and other back-office processes.

58. First Data, the largest merchant acquirer, issuer processor, and independent network services provider in the world, recommends two highly effective technologies available to address these two specific points of vulnerability: encryption and tokenization.[25] "Encryption

[25] *See* First Data Market Insight, *Avoiding a Data Breach: An Introduction to Encryption and Tokenization*, FIRST DATA CORP. (Aug. 22, 2013), https://www.firstdata.com/en_ie/insights/6203-Data-Breach-Market-Insight.html; *see also Point of Sale Security*, *supra* n.1.

mitigates security weaknesses that exist when [Payment Card Data] has been captured but not yet authorized. Tokenization addresses security vulnerabilities after a transaction has been authorized." *Id.* As First Data further explains:

> In the process of tokenization, once the transaction is authorized the payment data is sent to a centralized and highly secure server where it is stored. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The token number—which cannot be monetized by anyone but the merchant that owns the token—can be used in subsequent post-authorization business processes. . . . If token numbers are breached, they are meaningless to data thieves because they are simply random numbers. (*Id.*)

59. On information and belief, Hudson Bay failed to encrypt Plaintiffs' Payment Card Data within its POS terminals.

60. Had Hudson Bay employed certain best practices regarding encryption of Payment Card Data at the POS terminal, it could have prevented the use of stolen Payment Card Data.

3. Hudson Bay Failed to Install Software to Adequately Track and Monitor Its Network

61. Given that the window of intrusion lasted nearly a year, Hudson Bay failed to adequately track access to its network and to monitor the network for unusual activity, particularly with respect to its POS terminals, which would have allowed Hudson Bay to detect and potentially prevent hackers from stealing Payment Card Data.

62. One software vendor, Symantec Corporation ("Symantec"), provides the following explanation regarding its endpoint protection software: Symantec's network threat protection "technology analyzes incoming and outgoing traffic and blocks threats while they travel through the network before reaching endpoints. Rules-based firewall and browser protection defend against web-based attacks."[26]

---

[26] *Symantec Endpoint Protection Cloud*, SYMANTEC CORP. (2018), https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-cloud-en.pdf.

63. Specifically, had Hudson Bay implemented proper endpoint detection and prevention systems, it would have been able to identify suspicious activity occurring within its network. Additionally, proper endpoint detection would have triggered warnings and alerted Hudson Bay to the transmission of Payment Card Data within its systems and should have alerted Hudson Bay to large volumes of data being removed, or exfiltrated, from its network.

D. In Breaching Its Duty to Not Create Risk of Harm to Others, Hudson Bay Chose Not to Follow Industry Standards of Care

64. Hudson Bay's adherence to reasonable standards of care would have either prevented or timely detected this Data Breach. In addition to the best practices discussed above, industry groups and federal agencies have issued standards of care regarding adequate data security measures.

65. The Payment Card Industry Data Security Standard ("PCI-DSS") is a list of 12 information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI-DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted and requires merchants, like Defendants, to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

66. The 12 requirements of the PCI-DSS are:

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 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[27]

67. Furthermore, PCI-DSS 3.2.1 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

68. As the oldest operating company in North America, Hudson Bay was, at all times, fully aware of its data protection obligations in light of its daily collection and transmission of tens of thousands of sets of Payment Card Data.

69. In addition, the Department of Homeland Security and other security organizations provided Hudson Bay with warnings of POS system attacks. Specifically, U.S. CERT, part of the Department of Homeland Security, issued Alert TA14-002A on January 2, 2014, titled "Malware Targeting Point of Sale Systems."[28] The document discusses hardware and software attacks

---

[27] PCI Sec. Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1* at 9, 40 (July 2018), https://www.pcisecurity standards.org/documents/PCI_DSS-QRG-v3_2_1.pdf?agreement=true&time=1557938221691.

[28] Alert (TA14-002A), *supra* n.21.

against POS systems and includes specific best practices recommended to protect POS systems. *Id*.; *see also Tech Insight*, *supra* n.2.

70. The Cybersecurity Framework developed by National Institute of Standards and Technology ("NIST"), federal agency that works with industries to develop and apply technology, measurements, and standards, also provides businesses with guidance on best practices. The Cybersecurity Framework cites numerous industry standards available to guide businesses in adopting best practices, including the Information Systems Audit and Control Association's ("ISACA") Control Objectives for Information and Related Technology ("COBIT"), the Council on CyberSecurity's Top 20 Critical Security Controls, the International Society of Automation's Standards (such as ANSI/ISA-62443-2-1 (99.02.01)-2009 and ANSI/ISA-62443-3-3 (99.03.03)-2013), and the International Organization for Standardization's ISO/IEC 27001:2013.[29]

71. According to the *ISACA Journal*, the Enterprise Strategy Group found that 72% of North American organizations with 1,000 or more employees have implemented one or more formal IT best-practice control and process models and standards, such as COBIT and ISO/IEC 27001 and 27002.[30]

72. COBIT 5 provides management practices and monitoring processes to adequately protect organizations from internal and external data threats. *Id.* Specifically, COBIT 5 "Management Practices" recommend that organizations implement the following (*id.*):

---

[29] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, NAT'L INST. OF STANDARDS & TECH. (Feb. 12, 2014), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[30] Mathew Nicho, Ph.D., CEH, SAP-SA, RWSP, and Hussein Fakhry, Ph.D., *Using COBIT 5 for Data Breach Prevention*, 5 ISACA J. 23 (2013), https://www.isaca.org/Journal/archives/2013/Volume-5/Pages/Using-COBIT-5-for-Data-Breach-Prevention.aspx#2.

- "APO13.01 Establish and maintain an information security management system (ISMS)."
- "DSS05.01 Protect against malware."
- "DSS05.02 Manage network and connectivity security."
- "DSS05.03 Manage endpoint security."
- "DSS05.04 Manage user identity and logical access."
- "DSS05.05 Manage physical access to IT assets."

73. The ISO and the International Electrotechnical Commission ("IEC") have likewise developed standards and models for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security management systems. ISO/IEC 27001 sets forth a check list and control objectives for information security policies for organizations to protect their information systems and networks.[31] Specifically, the control objectives include:

> ***A.5.1 Information security policy***
>
> *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
>
> * * *
>
> A.6.1.1 Management commitment to information security
>
> *Control*
>
> Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
>
> ***A.10.3 System planning and acceptance***

[31] *ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements*, ISO/IEC (Oct. 15, 2005), http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf.

Objective: To minimize the risk of systems failures.

* * *

A.10.3.2 System acceptance

Control

Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

A.10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

A.10.4.1 Controls against malicious code

Control

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

* * *

A.10.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

A.10.6.1 Network controls

Control

Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

* * *

A.10.10 Monitoring

Objective: To detect unauthorized information processing activities.

A.10.10.1 Audit logging

Control

Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

* * *

A.11.4 Network access control

Objective: To prevent unauthorized access to networked services.

A.11.4.1 Policy on use of network services

Control

Users shall only be provided with access to the services that they have been specifically authorized to use.

* * *

A.11.4.7 Network routing control

Control

Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

* * *

A.12.4 Security of system files

Objective: To ensure the security of system files.

A.12.4.1 Control of operational software

Control

There shall be procedures in place to control the installation of software on operational systems.

* * *

A.13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

A.13.1.1 Reporting information security events

Control

Information security events shall be reported through appropriate management channels as quickly as possible. (*Id.* at 13-26.)

74. Similarly, ISO/IEC 27002 provides additional, specific best practice recommendations on information security management systems.[32] ISO 27002 states that in order to properly protect against malicious and mobile code and to protect the integrity of software and the organization's information, the following guidance should be observed: "Implementation guidance[:] Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls." *Id.* at 42.

75. Because Hudson Bay stores accepted payment cards containing sensitive financial and personal information, Defendants knew that financial institutions, such as Plaintiffs and the Class, were entitled to, and did, rely on Defendants to keep that sensitive information secure from would-be data thieves in accordance with at least the PCI-DSS requirements. Hudson Bay did not even meet this minimum standard of care, much less even attempt to comply with other well-known best practices.

E. Federal and State Statutes Create a Statutory Duty to Not Engage in Unfair Practices

1. The FTC Act and Similar State Statutes

76. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential

[32] *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management*, ISO/IEC (June 15, 2005), http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf.

consumer data, such as Payment Card Data, constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914, 15 U.S.C. §45 ("FTC Act").

77. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

78. The FTC also has published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[33]

79. The FTC also has issued numerous orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

80. In addition, individual states have enacted statutes based upon the FTC Act that also create a statutory duty to not engage in unfair business practices. Each statute is interpreted consistently with §5 of the FTC Act, with consideration given to the interpretation and construction given to §5 by the FTC and federal courts.

---

[33] Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business*, FTC.GOV (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

2. State Statutes Provide Guidance Regarding the Standard of Care Required to Protect Data

81. State law also provides guidance regarding the standard of care required to protect personal and financial information contained in the Payment Card Data that is acquired by and entrusted to businesses like Hudson Bay. *See* N.Y. Gen. Bus. Law §399-h. These statutes require businesses, like Hudson Bay, to implement and maintain reasonable security procedures and practices to protect the personal and financial information, which is contained in Payment Card Data, to prevent unauthorized access, destruction, use, modification, or disclosure of the information.

82. The FTC Act and its state law counterparts, at a minimum, provide a reasonable standard of care, if not a statutory duty, with which Hudson Bay did not even attempt to comply.

F. The Financial Losses that Financial Institutions Have Suffered, and Will Continue to Suffer, Were Foreseeable

83. Processing a payment card transaction involves four major steps:

- *Authorization* – when a customer presents a card to make a purchase, Hudson Bay requests authorization of the transaction from the card's issuer using the Payment Card Data from the card presented;
- *Clearance* – if the issuer authorizes the transaction, Hudson Bay completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays Hudson Bay for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

84. Payment Card Data is central to the payment card transaction process. For financial institutions, like Plaintiffs, Payment Card Data is an asset that has significant value. Payment Card Data is owned by the financial institution, not the cardholder; the cardholder is merely an authorized user. Payment Card Data is kept by financial institutions in the form of computer data, stored as records in a secured database on a financial institution's computer system.[34] In addition, the Payment Card Data is encoded on the magnetic stripe of the payment card. Payment Card Data is a financial institution's means of authenticating the cardholder and authorizing a payment card transaction.

85. To authorize a transaction, the issuing financial institution receives, from the merchant, the Payment Card Data that is encoded on the payment card being used by the consumer. The issuing financial institution's computer uses the Payment Card Data, received from the merchant, to locate the computer data on the financial institution's computer for the payment card's specific record. The financial institution then uses the payment card's specific record stored on its computer to authorize the transaction. The transaction authorization process relies on the Payment Card Data being known only to the parties to the payment card transaction.

86. When Payment Card Data (that is stored on financial institutions' computer systems and used to securely authorize financial transactions) is compromised, the computer database record that contains the compromised Payment Card Data is no longer usable to securely authorize

[34] "Each row of a database comprises a single record made up of multiple distinct pieces of information, and each column of the database table represents an attribute of that record." Dave Shackleford, *Regulations and Standards: Where Encryption Applies*, Sophos Ltd. (May 2014), https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/PublicSectorBenelux/sophos-encryption-regulations-standards-wpna.pdf. For example, a record of protected stored Payment Card Data for the financial institutions will include, but not be limited to, the following sensitive information: cardholder name; address; primary account numbers; and associated financial information, such as expiration date, daily limits, and service codes.

transactions. Due to the disclosure of the Payment Card Data to third parties, the computer data for the specific payment card becomes susceptible to fraud, and therefore, loses its integrity.

87. "Integrity" is a fundamental attribute of computer data. *See, e.g.*, 44 U.S.C. §3542(b)(1)(A) (defining integrity as an attribute of the federal government's information security policy). "Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or subversive conduct or acts contrary to what the system owner or privilege grantor intended. Integrity concerns computer data stored, processed, or in transit. In the context of databases, integrity also regards metadata and the functions involved."[35]

88. When a data breach occurs, the computer database record that contains the compromised Payment Card Data is damaged and no longer usable to authorize transactions. In other words, the financial institution can no longer count on the person using the information to be the cardholder and cannot rely on its computer data to securely authorize transactions. The Payment Card Data therefore effectively is rendered commercially worthless.

89. Thus, when Payment Card Data has lost its integrity, the financial institution must issue a replacement payment card with new Payment Card Data to prevent fraud. As a result, the computer data (database record) that contains the compromised Payment Card Data must be replaced with new computer data (database record) that matches the newly issued Payment Card Data.

90. These actions are not optional for financial institutions. For example, the Gramm-Leach-Bliley Act ("GLBA") mandates that financial institutions protect the security and confidentiality of consumer nonpublic personal information at all times. *See* 15 U.S.C. §§6801-9.

---

[35] Ioana Vasiu and Lucian Vasiu, Phd., MBA, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. PITT. J. TECH. L. & POL'Y 158, 160 (2014), https://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/139/149.

91. In short, Payment Card Data kept as computer data is Plaintiffs' and the Class's means of authenticating the cardholder and authorizing a transaction. When the Payment Card Data reflected in the computer data was compromised in the Data Breach, the computer data was damaged because it lost its integrity and Plaintiffs and the Class no longer could rely on it to authorize transactions. In other words, Plaintiffs and the Class no longer can count on the person using the information to be the cardholder and cannot rely on its computer data to securely authorize transactions. Therefore, Hudson Bay, by implementing inadequate data security measures, caused Plaintiffs and the Class to suffer damage.

92. The damage suffered by Plaintiffs and the Class was foreseeable to Defendants. Defendants knew that implementing data security measures that were inadequate to protect Payment Card Data would cause harm to the card-issuing institutions, such as Plaintiffs and the Class, because the issuers are financially responsible for fraudulent card activity (*see* 12 C.F.R. §§1005.6, 1026.12) and must incur significant costs to prevent additional fraud. Indeed, Defendants' public statement to customers after the Data Breach, which "encourages customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize[,]"[36] plainly indicates that Defendants believes that card-issuing institutions, like Plaintiffs and the Class, should be responsible for fraudulent charges on cardholder accounts resulting from the Data Breach.

93. As the direct and proximate result of Hudson Bay's conduct, Plaintiffs have suffered and will continue to suffer irreparable injury and significant financial losses. Specifically, Plaintiffs and other financial institutions have been forced to: (a) cancel or reissue any credit and debit cards identified by a payment card network as compromised in the Data Breach; (b) stop

[36] HBC Provides Information about Data Security Issue, *supra* n.13.

payments and block transactions from any deposit, transaction, checking, or other accounts that are linked to debit cards that were identified by a payment card network as compromised in the Data Breach or closing such accounts; (c) refund any cardholder for any unauthorized transaction on payment cards identified by a payment card network as compromised in the Data Breach; and (d) respond to a higher volume of cardholder complaints, confusion, and concern. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges are discovered and occur.

94. Moreover, Plaintiffs' and the Class's business is reliant on their reputation and customer relationships and their ability to maintain and grow their customer base in a competitive market. By engaging, and continuing to engage, in the conduct and activities described herein, Hudson Bay inevitably will be subject to a data breach again.

CLASS ACTION ALLEGATIONS

95. Plaintiffs bring Counts One, Two, Four, and Five below (the "Nationwide Claims") individually and on behalf of all other financial institutions similarly situated pursuant to Fed. R. Civ. P. 23. The proposed Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions − in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card-issuing services, whose customers made purchases from Hudson Bay stores from May 1, 2017, to March 31, 2018 (the "Class").

96. Plaintiff Summit FCU also brings Count Four below individually and on behalf of those defined below within the identified state pursuant to Fed. R. Civ. P. 23. The proposed statewide Class is defined as:

> All Financial Institutions − including, but not limited to, banks and credit unions – that are located in New York that issue payment cards, including credit and debit cards, or perform, facilitate, or support card-issuing services, whose customers made purchases from Hudson Bay stores from May 1, 2017, to March 31, 2018 (the "New York Class").

97. Excluded from each Class are Defendants and their subsidiaries, franchises, and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

98. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of each Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiffs. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

99. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3)'s predominance requirement are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

(a) whether Hudson Bay engaged in the misconduct alleged;

(b) whether Hudson Bay implemented data security measures that were inadequate to detect and potentially prevent the Data Breach and protect Payment Card Data;

(c) whether Hudson Bay owed a duty to Plaintiffs and Class members and whether Hudson Bay violated that duty;

(d) whether Hudson Bay engaged in unfair or unlawful acts and practices in violation of state consumer protection statutes;

(e) whether Plaintiffs and Class members were injured and suffered damages or other ascertainable loss as a result of Hudson Bay's conduct; and

(f) whether Plaintiffs and Class members are entitled to relief and the measure of such relief.

100. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Each Plaintiff is a member of the Class, having issued payment cards that were compromised in the Data Breach. Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct and Plaintiffs and each Class are asserting claims based on the same legal theories.

101. **Adequacy:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Each Plaintiff is an adequate Class representative because it is a member of the Class and its interests do not conflict with the interests of the other members of the Class that it seeks to represent. Each Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the Class's interests.

102. **Superiority:** The superiority requirement of Fed. R. Civ. P. 23(b)(3) is satisfied. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Hudson Bay, so it would be impracticable for members of the Class to individually seek redress for Hudson Bay's wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

103. **Injunctive and Declaratory Relief:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants, through their uniform conduct, acted, or refused to act, on grounds generally applicable to each Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

CHOICE OF LAW

104. New York has a significant interest in regulating the conduct of businesses operating within its borders. New York, which seeks to protect the rights and interests of New York and all residents, citizens, and businesses of the United States against a company headquartered and doing business in New York, has a greater interest in the Nationwide Claims of Plaintiffs and Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

105. HBC, which is the ultimate parent company for each of the other Defendants in this litigation, and owns Saks and Lord & Taylor stores, has its principal place of business in New York, New York. Defendants Saks and Lord & Taylor all have their principal place of business in New York, New York.

106. New York is the "nerve center" of Hudson Bay's business activities – the place where its high-level officers direct, control, and coordinate Hudson Bay's activities, including its data security functions and major policy, financial, and legal decisions.

107. Hudson Bay's acts, includings its breaches of duty to Plaintiffs and Class members, emanated from New York.

108. Hudson Bay's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in New York.

109. Under New York's choice of law principles, which are applicable to this action, the common law of New York applies to Plaintiffs' and the Class's Nationwide Claims.

110. Application of New York law to Plaintiffs' and the Class's Nationwide Claims is neither arbitrary nor fundamentally unfair because New York has significant contacts and a significant aggregation of contacts that create a state interest in Plaintiffs' and Class members' claims.

COUNT ONE
Negligence
(On Behalf of Plaintiffs and the Class)

111. Plaintiffs incorporate and reallege each and every allegation contained above as if fully set forth herein.

112. Defendants owed – and continue to owe – a duty to Plaintiffs and the Class to use and exercise reasonable care in obtaining and processing Plaintiffs' and the Class's Payment Card Data. This duty arises from the common law and statute and is independent of any duty Hudson Bay owed as a result of its contractual obligations.

113. Hudson Bay has an independent common law duty of reasonable care to prevent the foreseeable risk of harm to others, including Plaintiffs and the Class. It was entirely foreseeable to Hudson Bay that injury would result from the use of inadequate and unreasonable data security measures to protect Payment Card Data. It was also foreseeable that if reasonable security measures were not taken, hackers would steal Plaintiffs' and the Class's Payment Card Data; thieves would use Payment Card Data to make large numbers of fraudulent transactions; and as a

result, Plaintiffs and the Class would be required to replace the computer data rendered useless by the Data Breach, cancel and reissue the compromised payment cards, and reimburse their customers for any unauthorized transactions relating to the Data Breach.

114. Plaintiffs and the Class thus seek to recover for Hudson Bay's breach of an independent duty to not create unreasonable risk with regard to Plaintiffs' and the Class's Payment Card Data. Hudson Bay had a duty to employ reasonable data security measures because inadequate measures foreseeably create an unreasonable risk that Plaintiffs' and the Class's Payment Card Data would be compromised, with substantial financial loss resulting. In failing to maintain reasonable security measures, Hudson Bay created the risk of the harm that occurred and Plaintiffs and the Class were the foreseeable victims of that harm.

115. Defendants knew, or should have known, of the risk that its POS system could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

116. Defendants knew, or should have known, that their implementation of inadequate and unreasonable data security measures to protect its POS terminals against obvious risks would result in harm to Plaintiffs and the Class.

117. By accepting payment cards, Hudson Bay also voluntarily assumed the duty to use reasonable security measures. When a company, such as Hudson Bay, through the ordinary course of its business (and for its own economic benefit) receives, gathers, and/or stores Payment Card Data, it has undertaken to render services necessary for the protection of that Payment Card Data, and therefore has an affirmative duty to take reasonable efforts to provide security for that Payment Card Data.

118. A duty to use reasonable security measures also arose as a result of the special relationship that existed between Hudson Bay and Plaintiffs and the Class. The special relationship arose because financial institutions entrusted Hudson Bay with Payment Card Data from payment cards they issued. Only Hudson Bay was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

119. Moreover, §5 of the FTC Act imposes a statutory duty on merchants to not engage in unfair business practices, which the FTC repeatedly has determined includes the duty to use reasonable data security measures. In addition, individual states have enacted statutes based on the FTC Act, as alleged herein, that also create a statutory duty to not engage in unfair business practices.

120. Defendants breached their common law and statutory duties when they knowingly: (a) ignored well-known data security risks, thereby intentionally allowing data security deficiencies to persist; (b) refused to implement certain protocols, such as end-to-end encryption, that would have protected Payment Card Data; and (c) failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of the hacker and prevented Payment Card Data from being stolen.

121. But for Hudson Bay's unreasonable and inadequate data security measures, Plaintiffs' and the Class's Payment Card Data would not have been compromised. Among other things, had Hudson Bay employed end-to-end encryption, Plaintiffs' and the Class's Payment Card Data would not have been compromised.

122. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and the Class have suffered, and continue to suffer, substantial financial losses, as detailed herein.

COUNT TWO
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

123. Plaintiffs incorporate and reallege each and every allegation contained above as if fully set forth herein.

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Hudson Bay, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Hudson Bay's duty.

125. Hudson Bay violated §5 of the FTC Act (and similar state statutes) by implementing unreasonable data security measures that were inadequate to protect Payment Card Data. Hudson Bay's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at an international restaurant, including, specifically, the immense damages that would result to consumers and financial institutions.

126. Hudson Bay's violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

127. Plaintiffs and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses and maintaining the confidentiality of Payment Card Data. Moreover, both Plaintiffs and many Class members are credit unions, which are organized as cooperatives, whose members are consumers.

128. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures

and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

129. As a direct and proximate result of Hudson Bay's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, substantial financial losses, as detailed herein.

COUNT THREE
Violation of New York General Business Law,
N.Y. Gen. Bus. Law §§349, *et seq.*
(On Behalf of Plaintiff Summit FCU and the New York Class)

130. Plaintiff Summit FCU incorporates and realleges each and every allegation contained above as if fully set forth herein.

131. New York General Business Law §349 ("GBL §349") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Plaintiff Summit FCU and the New York Class are financial institutions located in New York, which extend the credit that facilitates economic growth in New York and therefore rely on the integrity of the credit reporting industry.

132. Hudson Bay's deceptive acts and practices complained of herein were consumer oriented and impacted the public at large, including the New Yorkers affected by the Data Breach, and the banks and credit unions headquartered in New York that were affected by the Data Breach. Hudson Bay repeatedly engaged in the deceptive acts and practices complained of herein, and repreatedly deceived Plaintiff Summit FCU, members of the New York Class, and the public at large regarding the adequacy and reasonableness of its data security measures, ability to secure Payment Card Data, and compliance with the PCI-DSS requirements.

133. In the conduct of Hudson Bay's business, trade, commerce, or in the furnishing of services, Hudson Bay misrepresented that it would protect Plaintiff Summit FCU's and members of the New York Class's Payment Card Data, including by maintaining reasonable security

measures. By accepting payment cards, Hudson Bay misrepresented to Plaintiff Summit FCU and members of the New York Class that it was PCI-DSS compliant.

134. In the conduct of Hudson Bay's business, trade, commerce, or in the furnishing of services, Hudson Bay failed to disclose to Plaintiff Summit FCU or members of the New York Class that it did not maintain adequate or reasonable data security measures, did not secure Payment Card Data, and was not PCI-DSS compliant. Hudson Bay's omissions were material to Plaintiff Summit FCU and members of the New York Class because had Hudson Bay disclosed that its data systems were not secure, and thus, vulnerable to attack, Hudson Bay would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

135. Hudson Bay's deceptive acts or practices were likely to deceive reasonable financial institutions about the adequacy of Hudson Bay's data security measures and its ability to protect Plaintiff Summit FCU's and members of the New York Class's Payment Card Data. Plaintiff Summit FCU and members of the New York Class had no way of learning about Hudson Bay's deceptive acts or practices because Hudson Bay had near exclusive control over information regarding its security measures and the safety of its POS systems and cardholder data environment.

136. As a direct and proximate result of Hudson Bay's deceptive acts and practices, Plaintiff Summit FCU and New York Class members have suffered, and will continue to suffer, injury, ascertainable losses of money, and monetary and non-monetary damages.

137. Plaintiff Summit FCU and New York Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

COUNT FOUR
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

138. Plaintiffs incorporate and reallege each and every allegation contained above as if fully set forth herein.

139. Plaintiffs bring this claim individually and on behalf of the Class under the law of New York. Although there are numerous permutations of the elements of the unjust enrichment cause of action in the various states, there are a few real differences. In all states, the focus of an unjust enrichment claim is whether the defendant was unjustly enriched. At the core of each state's law are two fundamental elements – the defendant received a benefit from the plaintiff; and it would be inequitable for the defendant to retain that benefit without compensating the plaintiff. The focus of the inquiry is the same in each state. Since there is no material conflict relating to the elements of unjust enrichment between the different jurisdictions from which Class members will be drawn, the law of New York applies to the claims of the Class.

140. Plaintiffs and members of the Class enriched Hudson Bay by conferring upon it the non-gratuitous benefit of allowing their payment cards to be accepted at Hudson Bay's stores. These non-gratuitous benefits were conferred at Plaintiffs' and the Class's expense. Plaintiffs and members of the Class would not have allowed their payment cards to be accepted at Hudson Bay's stores had Hudson Bay disclosed to Plaintiffs and the Class that its data systems were not secure and, thus, vulnerable to attack. Had Hudson Bay disclosed that its data systems were not secure and, thus, vulnerable to attack, Hudson Bay would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

141. Hudson Bay had knowledge of and appreciated the non-gratuitous benefits conferred by Plaintiffs and members of the Class by appreciating revenues derived from the purchases of merchandise that were made using Plaintiffs' and Class members' Payment Card

Data. Hudson Bay knew both that a substantial portion of its sales were attributable to credit and debit card transactions and it was appreciating revenues derived from such sales, even though it had failed to maintain adequate data security measures, adhere to the PCI-DSS requirements, or otherwise protect Plaintiffs' and the Class's Payment Card Data.

142. Hudson Bay accepted or retained the non-gratuitous benefits conferred by Plaintiffs and members of the Class.

143. It would be unjust and inequitable to allow Hudson Bay to retaining the non-gratuitous benefits conferred upon Hudson Bay by Plaintiffs and the Class under these circumstances. Hudson Bay was solely responsible for securing its networks and protecting Plaintiffs' and Class's Payment Card Data and there was no way Plaintiffs or Class members could have known about Hudson Bay's inadequate data security practices or avoided the injuries they sustained. Thus, Hudson Bay must pay restitution to Plaintiffs and members of the Class for unjust enrichment, as ordered by the Court.

COUNT FIVE
Request for Declaratory and Injunctive Relief
(On Behalf of Plaintiffs and the Class)

144. Plaintiffs incorporate and reallege each and every allegation contained above as if fully set forth herein.

145. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and violate the terms of the federal and state statutes described herein.

146. An actual controversy has arisen in the wake of the Data Breach regarding Hudson Bay's duty to reasonably safeguard Payment Card Data. Plaintiffs allege that Hudson Bay's data security measures were inadequate and remain inadequate. Hudson Bay likely will deny these

allegations. Furthermore, Plaintiffs and the Class continue to suffer injury as additional fraudulent charges are being made on payment cards issued to Hudson Bay customers.

147. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

(a) Hudson Bay continues to owe a legal duty to secure Payment Card Data;

(b) Hudson Bay continues to breach this legal duty by employing inadequate and unreasonable measures to secure Payment Card Data; and

(c) Hudson Bay's ongoing breaches of its legal duty continue to cause harm to Plaintiffs and the Class.

148. The Court also should issue corresponding injunctive relief requiring Hudson Bay to employ adequate security protocols, consistent with industry standards, to protect Plaintiffs' and the Class's Payment Card Data. Specifically, this injunction should, among other things, direct Hudson Bay to:

(a) utilize industry standard encryption to encrypt the transmission of cardholder data at POS and at all other times;

(b) implement encryption keys in accordance with industry standards;

(c) engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

(d) audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

(e) regularly test its systems for security vulnerabilities, consistent with industry standards; and

(f) comply with all PCI-DSS standards pertaining to the security of its customers' personal and confidential information.

149. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Hudson Bay. The risk of another such breach is real, immediate, and substantial. Indeed, Hudson Bay is a recidivist, having already allowed third parties to access unecrypted customer information in 2017. If another breach at Hudson Bay occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for out-of-pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable and reputational damage.

150. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Hudson Bay, if an injunction is issued. Among other things, if another massive data breach occurs at Hudson Bay, Plaintiffs and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Hudson Bay of complying with an injunction, by employing reasonable data security measures, is relatively minimal and Hudson Bay has a pre-existing legal obligation to employ such measures.

151. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Hudson Bay, thus eliminating the injuries that would result to Plaintiffs and the Class whose Payment Card Data would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request that this Court enter a judgment against Defendants and in favor of Plaintiffs and the Class and award the following relief:

A. That this action be certified as a class action, pursuant to Fed. R. Civ. P. 23, declaring Plaintiffs as representatives of the Class and Plaintiffs' counsel as counsel for the Class;

B. Monetary damages;

C. Injunctive relief;

D. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. Costs;

F. Pre- and post-judgment interest; and

G. Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs, individually and on behalf of the Class, demand a trial by jury for all issues so triable.

DATED: December 3, 2019

SCOTT+SCOTT ATTORNEYS AT LAW LLP

/s/ Joseph P. Guglielmo
Joseph P. Guglielmo
Carey Alexander
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: 212-223-6444
Facsimile: 212-223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com

Erin Green Comite
SCOTT+SCOTT ATTORNEYS AT LAW LLP
156 South Main Street

Colchester, CT 06415
Telephone: 860-537-5537
Facsimile: 860-537-4432
ecomite@scott-scott.com

Karen S. Halbert
Michael L. Roberts
Jana K. Law
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223
Telephone: 501-821-5575
Facsimile: 501-821-4474
karenhalbert@robertslawfirm.us
mikeroberts@robertslawfirm.us
janalaw@robertslawfirm.us

Gary F. Lynch
CARLSON LYNCH LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: 412-322-9243
Facsimile: 412-231-0246
glynch@carlsonlynch.com

Attorneys for Plaintiffs Arkansas Federal Credit Union and The Summit Federal Credit Union