IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE

JEANNE SACKLOW and ERIKA TARGUM, individually and on behalf of all others similarly situated,	)	Civil Action No.:
Plaintiffs,	)	**COMPLAINT--CLASS ACTION**
v.	)	**JURY TRIAL DEMANDED**
SAKS INCORPORATED,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiffs Jeanne Sacklow and Erika Targum ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts respectively pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against defendant Saks Incorporated ("Defendant" or "Saks").

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Saks for its failure to exercise reasonable care in securing and safeguarding its customers' personal financial data—in particular, credit and debit card records including cardholder name, card number, expiration date, and internal verification code ("Private Information").

2. On March 28, 2018, a criminal syndicate known as "Joker's Stash" announced the release for sale on the dark web of over five million stolen credit and debit card records. The cybersecurity firm Gemini Advisory determined that the cards were misappropriated in a breach involving Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor retail stores during the period between no later than May 2017 and late-March 2018 ("Security Breach").

3. On April 1, 2018, Saks announced that it "became aware of a data security issue involving customer payment card data."

4. On information and belief, Plaintiffs' and Class members' Private Information was stolen by hackers in order to be sold on the dark web when Plaintiffs and Class members used their credit and debit cards at Saks stores.

5. Saks' security failures enabled the hackers to steal Plaintiffs' and Class members' Private Information. The failures put Plaintiffs' and Class members' financial information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members attributable to responding to, identifying, and correcting damages that were reasonably foreseeable as a result of Saks' willful and negligent conduct. The hackers will continue to sell the Private Information—and various cyber criminals will continue to buy and use it—in order to exploit and injure Plaintiffs and Class members across the United States.

6. The Security Breach was caused and enabled by Saks' knowing violation of its obligations to abide by best practices and industry standards concerning the security of payment systems. Saks failed to comply with security standards and allowed its customers' financial information and other Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Security Breach that occurred.

7. Accordingly, Plaintiffs, on behalf of themselves and other members of the Class, assert claims for breach of implied contract, negligence, and unjust enrichment, and seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

II. JURISDICTION AND VENUE

8. The Court has jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a

citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

9. The Court has personal jurisdiction over Saks Incorporated because Saks is a Tennessee corporation.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and 1391(c)(2) because Saks Incorporated is a Tennessee corporation and is subject to personal jurisdiction in this district.

III. PARTIES

11. Plaintiff Jeanne Sacklow is a citizen of the State of New York. In March of 2018, she used her credit card to make a purchase at a Saks Fifth Avenue store in New York City, and had her Private Information exposed as a result of Saks' inadequate security. As a result of the Security Breach, she spent time inspecting her credit card statements for fraudulent activity. She has also suffered from the deprivation of the value of her Private Information and the lost benefit of the bargain.

12. Plaintiff Erika Targum is a citizen of the State of New York. In May of 2017, she used a credit card to return a purchase to a Saks Fifth Avenue store in New York City, and had her Private Information exposed as a result of Saks' inadequate security. As a result of the Security Breach, she spent time inspecting her credit card statements for fraudulent activity. She has also suffered from the deprivation of the value of her Private Information and the lost benefit of the bargain.

13. Saks Incorporated is a Tennessee Corporation which operates a number of luxury department stores selling clothing, footwear, jewelry, beauty products, fragrances, electronics, bedding, and housewares.

IV. FACTUAL BACKGROUND

14. Saks uses a payment system to electronically process its customers' credit and debit card payments. In the years preceding Saks' announcement of the Security Breach, several retail outlets made announcements alerting the public of security breaches at their stores, including Barnes & Noble, Home Depot, Neiman Marcus, Michaels, Target, and TJ Maxx. Saks knew or should have known that its customers' card data was squarely within the crosshairs of hackers. Despite this, Saks failed to take adequate steps to secure the payment system used in its stores.

The Saks Security Breach

15. On March 28, 2018, a criminal syndicate known as "Joker's Stash" announced that it would be releasing for sale on the dark web over five million stolen credit and debit card records.

16. "Joker's Stash" is a criminal syndicate trading in stolen debit and credit card data. Since its inception in 2014, Joker's Stash has attracted dozens of identity thief customers who have spent tens and hundreds of thousands of dollars on stolen credit card information.[1] As described by security researcher Brian Krebs, Joker's Stash offers its identity thief customers "loyalty programs, frequent-buyer discounts, money-back guarantees and just plain old good customer service."[2]

17. The cybersecurity firm Gemini Advisory determined that the card records being advertised for sale by Joker's Stash were stolen from a breach involving Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor retail stores during the period between May 2017 and late-March 2018.

18. The image below reflects a portion of Joker's Stash's advertisement for the stolen

[1] https://krebsonsecurity.com/2016/03/carders-park-piles-of-cash-at-jokers-stash/ (last visited April 4, 2018).
[2] *Id.*

Private Information describing the card records as including "TR1" and "TR2" data, which includes cardholder names, card numbers, expiration dates, and internal verification codes.

19. On April 1, 2018, nearly a year after hackers first began collecting the Private Information of Plaintiffs and other Class members, Saks announced that it "became aware of a data security issue involving customer payment card data." Saks' announcement misleadingly states that "We want to assure our customers that they will not be liable for fraudulent charges that may result from this matter"—without announcing any intention that Saks will itself compensate its customers for their damages.[3]

20. Saks' treatment of Private Information entrusted to it by its customers fell far short of satisfying its legal duties and obligations. Saks failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings, and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

21. Federal and State governments have likewise established security standards and

[3] https://www.saksfifthavenue.com/include/aem/aem_static.jsp?page=security-information-notice&site_refer=EML (last visited April 9, 2018).

issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[4]

22. In 2016, the Federal Trade Commission ("FTC") updated its publication, *Protecting Personal Information: A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[5] The guidelines note 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 network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting 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.

23. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[6]

---

[4] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 4, 2018).
[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 4, 2018).
[6] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 4, 2018).

24. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

25. In this case, Saks was at all times fully aware of its obligation to protect the Private Information of its customers because of its participation in payment card processing networks. Saks was also aware of the significant repercussions if it failed to do so because it collected payment card data from thousands of customers daily at its stores and Saks knew that this data, if hacked, would result in injury to consumers, including Plaintiffs and Class members.

26. As a result of Saks' failure to adhere to industry and government standards for the security of card data, Private Information of thousands of Saks customers, including Plaintiffs, was compromised over a time period spanning nearly one year.

Security Breaches Lead to Identity Theft

27. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.[7]

[7] *See Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 4, 2018).

28. Similarly, the FTC cautions that identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[8] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[9]

29. Private Information—which includes Plaintiffs' and Class members' names combined with their credit or debit card information that were stolen in the Security Breach at issue in this action—is a valuable commodity to identity thieves. Plaintiffs' and Class members' personal information is being sold and traded by cyber criminals on the dark web. Criminals often trade the information on the dark web for a number of years.

30. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[10] Private information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing

---

[8] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited April 4, 2018).

[9] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[10] Erika McCallister, et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited April 4, 2018).

that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

31. Private information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scopes to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

The Monetary Value of Privacy Protections and Private Information

32. The fact that Plaintiffs' and Class members' Private Information was stolen in order to be sold on the dark web—and is presently offered for sale to cyber criminals on the dark web—demonstrates the monetary value of the Private Information.

33. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[11]

34. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[12]

[11] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited April 4, 2018).

[12] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited April 4, 2018).

35. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[13]

36. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[14] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

37. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[15]

38. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Credit card numbers range in cost from $1.50 to $90 per card number.[16] By way of

---

[13] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited April 4, 2018).
[14] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited April 4, 2018).
[15] See Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 4, 2018).
[16] *The Cyber Black Market: What's Your Bank Login Worth*, available at https://leapfrogservices.com/the-cyber-black-market-whats-your-bank-login-worth/ (last visited April 4, 2018).

the Security Breach, Saks has deprived Plaintiffs and Class members of the substantial value of their Private Information.

39. Given these facts, any company that transacts business with consumers and then compromises the privacy of consumers' Private Information has thus deprived consumers of the full monetary value of their transaction with the company.

Damages Sustained by Plaintiffs and Class Members

40. A portion of the services purchased from Saks by Plaintiffs and the other Class members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Private Information, including their credit and debit card information. The cost to Saks of collecting and safeguarding Private Information is built into the price of all of its services. Because Plaintiffs and the other Class members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and the other Class members incurred actual monetary damages in that they overpaid for their purchases at Saks stores.

41. Plaintiffs and the other members of the Class have suffered additional injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) improper disclosure of their Private Information, which is now in the hands of criminals; (iii) the value of their time spent mitigating the increased risk of identity theft and identity fraud; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market—for which they are entitled to compensation.

42. Plaintiffs and the other Class members suffered additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend to monitor their financial accounts as a result of the Security Breach.

43. Acknowledging the damage to Plaintiffs and Class members, Saks is instructing customers who used their card at its stores to take certain cautionary steps. Credit and debit card users should review their accounts for unauthorized transactions and notify their banks immediately if they discover any unauthorized purchases or cash advances. Plaintiffs and the other Class members now face a greater risk of identity theft.

V. CLASS ACTION ALLEGATIONS

44. Plaintiffs bring all counts, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class defined as:

> All persons who used their credit, debit, or prepaid debit card at a Saks Fifth Avenue or Saks OFF 5th store during the period from May 2017 through March 2018.

Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

45. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

46. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, Class members number in the tens if not hundreds of thousands.

47. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Saks failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffs' and Class members' Private Information;

b. Whether Saks properly implemented its purported security measures to protect Plaintiffs' and Class members' Private Information from unauthorized capture, dissemination, and misuse;

c. Whether Saks took reasonable measures to determine the extent of the Security Breach after it first learned of the same;

d. Whether Saks' conduct constitutes breach of an implied contract;

e. Whether Saks willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Private Information;

f. Whether Saks was negligent in failing to properly secure and protect Plaintiffs' and Class members' Private Information;

g. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

48. Saks engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other Class members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

49. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were similarly injured through Saks' uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to Saks that are unique to Plaintiffs.

50. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiffs and their counsel.

51. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Saks. The Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

52. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** 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 Saks, so it would be impracticable for Class members to individually seek redress for Saks' 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 a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS

COUNT I
Negligence

53. Plaintiffs incorporate the preceding paragraphs 1 - 52 as if fully set forth herein.

54. Saks owes numerous duties to Plaintiffs and the other members of the Class. These duties include:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and the other members of the Class of the Security Breach.

55. Saks knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure payment systems. Saks knew or should have known of the many breaches that targeted other retail stores in the years before the Security Breach.

56. Saks knew or should have known that its payment systems did not adequately safeguard Plaintiffs' and the other Class members' Private Information.

57. Saks breached the duties it owes to Plaintiffs and Class members in several ways, including:

a. failing to implement adequate security systems, protocols and practices sufficient to protect customer Private Information and thereby creating a foreseeable risk of harm;

b. failing to comply with the minimum industry data security standards during the period of the data breach; and

c. failing to timely and accurately disclose to customers that their Private Information had been improperly acquired or accessed.

58. Saks was negligent in transmitting Plaintiffs' and the other Class members' Private Information over compromised electronic networks it had control over and should have known were compromised or susceptible to compromise.

59. But for Saks' wrongful and negligent breach of the duties it owed to Plaintiffs and the other Class members, their Private Information would not have been compromised.

60. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Saks' negligent conduct.

COUNT II
Breach of Implied Contract

61. Plaintiffs incorporate the preceding paragraphs 1 – 60 as if fully set forth herein.

62. In using credit or debit cards at Saks stores, Plaintiffs and the other members of the Class entered into an implied contract with Saks, whereby Saks became obligated to reasonably safeguard Plaintiffs' and the other Class members' Private Information.

63. Under the implied contract, Saks was obligated to not only safeguard the Private Information, but also to provide Plaintiffs and the other Class members with prompt, truthful, and adequate notice of any security breach or unauthorized access of said information.

64. Saks breached the implied contract with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their Private Information.

65. Saks also breached its implied contract with Plaintiffs and the other Class members by failing to provide prompt, truthful, and adequate notice of the Security Breach and unauthorized access of their Private Information by hackers.

66. Plaintiffs and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their Private Information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and identity fraud pressed upon them by the Security Breach; (iii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud; (iv) the increased risk of identity theft; and (v) deprivation of the value of their Private Information, which is likely to be sold to cyber criminals on the dark web. At the very least, Plaintiffs and the other Class members are entitled to nominal damages.

COUNT III
Unjust Enrichment

67. Plaintiffs incorporate the preceding paragraphs 1– 66 as if fully set forth herein.

68. Plaintiffs and the other Class members conferred a monetary benefit on Saks. Specifically, Plaintiffs and the other Class members paid for goods sold by Saks and provided Saks with payment information. In exchange, Plaintiffs and the other Class members were entitled to have Saks protect their Private Information with adequate data security.

69. Saks knew that Plaintiffs and the other Class members conferred a benefit on Saks. Saks profited from Plaintiffs' and the other Class members' purchases and used their Private Information for business purposes.

70. Saks failed to secure Plaintiffs' and the other Class members' Private Information and therefore did not provide full compensation for the benefit the Plaintiffs and the other Class members provided. Saks inequitably acquired the Private Information because it failed to disclose its inadequate security practices.

71. If Plaintiffs and the other Class members knew that Saks would not secure their Private Information using adequate security, they would not have shopped at Saks stores.

72. Plaintiffs and the other Class members have no adequate remedy at law.

73. Under the circumstances, it would be unjust for Saks to be permitted to retain any of the benefits that Plaintiffs and the other Class members conferred on it.

74. Saks should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and the other Class members proceeds that it unjustly received from them. In the alternative, Saks should be compelled to refund the amounts that Plaintiffs and the other Class members overpaid.

COUNT IV
Negligence Per Se

75. Plaintiffs incorporate the preceding paragraphs 1 – 74 as if fully set forth herein.

76. 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 Saks, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Saks' duty in this regard.

77. Saks violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described herein. Saks' conduct was particularly unreasonable given the nature and amount of Private Information its stores obtained and stored, and the foreseeable consequences of a data breach at a retail chain as large as Saks, including, specifically, the damages that would result to Plaintiffs and Class members.

78. Saks' violation of Section 5 of the FTC Act constitutes negligence *per se*.

79. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

80. The harm that occurred as a result of the Security Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued 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.

81. As a direct and proximate result of Saks' negligence *per se*, Plaintiffs and the Class will suffer injuries, including: inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Security Breach; false or fraudulent charges stemming from the Security Breach, including but not limited to late fees charged and forgone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Security Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may

take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

VII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Saks, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' motion for class certification;

B. Ordering Saks to pay actual damages to Plaintiffs and the other members of the Class;

C. Ordering Saks to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

D. Ordering Saks to pay attorneys' fees and litigation costs to Plaintiffs;

E. Ordering Saks to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief;

F. Ordering Saks to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: April 11, 2018

Respectfully submitted,

Jeanne Sacklow and Erika Targum, individually and on behalf of all others similarly situated,

/s/ Kevin H. Sharp

Kevin H. Sharp
Tennessee Bar No. 16287
SANFORD HEISLER SHARP, LLP
611 Commerce Street
Suite 3100
Nashville, TN 37203
Tel: (615) 434-7000
Fax: (615) 434-7020
ksharp@sanfordheisler.com

Ben Barnow*
Illinois Bar No. 0118265
Erich P. Schork*
Illinois Bar No. 6291153
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

Janine Pollack*
Daniel Tepper*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ, LLP
270 Madison Avenue
New York, New York 10016
Tel.: (212) 545-4600
Fax: (212) 686-0114
pollack@whafh.com
tepper@whafh.com

* *pro hac vice* application forthcoming

JS 44 (Rev. 07/16)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

JEANNE SACKLOW and ERIKA TARGUM, individually and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff New York County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Kevin Sharp; Sanford Heisler Sharp, LLP; 611 Commerce St., Ste. 3100 Nashville, TN 37203; (615) 434-7001 (see attached)

DEFENDANTS

SAKS INCORPORATED

County of Residence of First Listed Defendant New York County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ❒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. Section 1332(d)(2) and Section 1391

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE 04/11/2018

SIGNATURE OF ATTORNEY OF RECORD /s/ Kevin Sharp

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Attachment to Civil Cover Sheet

I.

(c) Attorneys for Plaintiffs

Kevin H. Sharp
SANFORD HEISLER SHARP, LLP
611 Commerce Street, Suite 3100
Nashville, Tennessee 37203
Telephone: (615) 434-7001
Facsimile: (615) 434-7020
Email: ksharp@sanfordheisler.com

Ben Barnow*
Erich P. Schork*
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312) 641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com

Janine Pollack*
Daniel Tepper*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ, LLP
270 Madison Avenue
New York, New York 10016
Tel.: (212) 545-4600
Fax: (212) 686-0114
pollack@whafh.com
tepper@whafh.com

* pro hac vice application forthcoming

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: Saks Joins Lord & Taylor in Facing Class Action Litigation Over Data Breach Affecting 5M Consumers