IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ANDE KYLES and DIANE TAYLOR, on behalf of themselves and all others similarly situated, Plaintiffs, v. STEIN MART, INC., a Florida corporation, and SOCIAL ANNEX, INC. (d/b/a, ANNEX CLOUD), a Delaware corporation, Defendants.	CASE NO. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Ande Kyles and Diane Taylor ("Plaintiffs") individually and on behalf of all others similarly situated, upon personal knowledge of the facts 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 Defendants Stein Mart, Inc. ("Stein Mart") and Social Annex, Inc. ("Annex") (together with Stein Mart, "Defendants").

NATURE OF THE ACTION

1. Plaintiffs bring this action, individually and on behalf of all others similarly situated whose sensitive financial and personal non-public information, including but not limited to their (a) names; (b) addresses; (c) email addresses; and (d) payment card information (including, *inter alia*, card numbers, expiration dates, and security codes ("CVV numbers")) (collectively, "Personal Information") was accessed and captured from Defendants' systems by unauthorized users during at least four of the following different periods of time between

December 28, 2017 and July 9, 2018: May 19, June 1, June 5, and July 8-9 2018 (the "Data Breach").

2. As alleged in greater detail below, Annex is a company that provides a service used by websites that enable consumers to use their user name and password from other websites—such as Facebook and Amazon—to log in to internet merchants' websites, such as Stein Mart's, to make online purchases thereon.

3. On or around November 13, 2018, Stein Mart sent letters to customers/consumers informing them that Annex's system was accessed by unauthorized users who were able to capture customers'/consumers' Personal Information, including payment card information, entered while making online purchases on Stein Mart's website.

4. As alleged herein, Defendants' failure to implement or maintain adequate data security measures for customers' information, including Personal Information, directly and proximately caused injuries to Plaintiffs and the Class (defined below).

5. Defendants failed to take reasonable steps to employ adequate security measures or to properly protect sensitive payment Personal Information despite well-publicized data breaches at large national retail and restaurant chains in recent years, including Arby's, Wendy's, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Dairy Queen, Kmart, and many others.

6. The Data Breach was the inevitable result of Defendants' inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite the fact that these types of data breaches were and are occurring throughout the restaurant and retail

industries, Defendants failed to ensure that they maintained adequate data security measures, causing customers' Personal Information to be stolen and/or accessed by unauthorized users.

7. As a direct and proximate consequence of Defendants' negligence and/or failure to implement and maintain adequate security measures, a massive amount of information was stolen from Defendants. Upon information and belief, the Defendants Data Breach compromised the Personal Information of thousands (if not more) of Defendants' customers/clients. Victims of the Data Breach have had their Personal Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

8. Moreover, Plaintiffs and Class Members have been forced to spend significant time associated with, among other things, detecting and expending effort to recuperate fraudulent charges on their debit and credit cards, cancelling/closing and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, and/or other losses resulting from the unauthorized use of their cards or accounts.

9. Rather than providing meaningful assistance to consumers to help deal with the fraud that has and will continue to result from the Data Breach, Defendants simply told them to carefully monitor their accounts. In contrast to what is and has been frequently made available to consumers in recent data breaches, Defendants have not offered or provided any monitoring service or fraud insurance to date.

10. Plaintiffs and Class Members seek to recover damages caused by Defendants' negligence, negligence *per se*, breach of implied contract, unjust enrichment and violations of

state consumer protection and data privacy statutes. Additionally, Plaintiffs seek declaratory and injunctive relief as a result of the conduct of Defendants discussed herein.

PARTIES

Plaintiff Diane Taylor

11. Plaintiff Diane Taylor is an adult residing in Denmark, South Carolina. On or about November 13, 2018, Plaintiff Taylor received a letter from Stein Mart informing her that it was subject to "a recent security incident involving some of [her] Personal Information that was maintained on [Defendants'] website." The letter claims to have been sent to inform her "about an incident involving one of [its] third-party vendors, Annex Cloud, that may involve some of [her] information," and that "Annex Cloud informed Stein Mart that they had detected and removed unauthorized code that had been added to the code used by Annex Cloud to enable logins … and could have captured information entered during the checkout process by customers who placed or attempted to place orders on [Stein Mart's] website."

12. Stein Mart's letter acknowledged the very real threat that the Data Breach would result in fraudulent charges, identity theft, and other similar risks by further instructing Plaintiff Taylor to "closely review [her] payment card statements for any unauthorized charges":

> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Information on additional steps you can take can be found on the following pages.
>
> We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we removed the Annex Cloud login feature from our website while the investigation is ongoing.

13. Although the letter was dated November 13, 2018, it stated that Stein Mart "sought additional information" from Annex "through October 25, 2018," which indicates that

both Stein Mart and Annex were aware of the Data Breach at least three weeks prior to sending letters to consumers informing them of its occurrence.

14. Moreover, the Vermont Office of Attorney General's website contains a letter from Stein Mart nearly identical to the one sent to Plaintiff Taylor dated September 14, 2018, which indicates that both Stein Mart and Annex were aware of the Data Breach at least as of that date.

15. During May 2018, Plaintiff Taylor received a notification from Bank of America that there had been fraudulent activity on her debit card. Upon immediately checking the transaction history of her banking account with Bank of America, Plaintiff Taylor determined and confirmed with Bank of America that two fraudulent charges had been made on her account.

16. The debit card used to make the fraudulent charges was the same one Plaintiff Taylor used to make purchases on Stein Mart's website, www.SteinMart.com.

17. On or about May 9, 2018, Bank of America cancelled the debit card associated with Plaintiff Taylor's checking account and mailed her a new debit card.

18. Prior to the fraudulent transactions discovered in May of 2018, Plaintiff Taylor had not experienced credit card fraud or identity theft with respect to her debit card. Furthermore, Plaintiff Taylor does not have a previous history of being victimized by payment card fraud.

19. Although Plaintiff Taylor was ultimately refunded her stolen money, as a result of having been victimized by the Data Breach, Plaintiff Taylor was required to spend time addressing the unauthorized transactions.

20. Had Plaintiff Taylor known that Defendants would not adequately protect the Personal Information and other sensitive information entrusted to them, she would not have made purchases on Stein Mart's online website using her debit card.

21. Had Plaintiff Taylor known that Defendants would not adequately protect the Personal Information and other sensitive information entrusted to them, she would not have transmitted her Personal Information to Defendants and/or allowed Defendants to store her Personal Information.

22. As a result of Defendants' failure to adequately safeguard Plaintiff Taylor's Personal Information, Plaintiff Taylor has been injured.

Plaintiff Ande Kyles

23. Plaintiff Ande Kyles is an adult residing in Florissant, Missouri. On or about November 13, 2018, Plaintiff Kyles received a letter from Stein Mart informing her that it was subject to "a recent security incident involving some of [her] Personal Information that was maintained on [Defendants'] website." The letter claims to have been sent to inform her "about an incident involving one of [its] third-party vendors, Annex Cloud, that may involve some of [her] information," and that "Annex Cloud informed Stein Mart that they had detected and removed unauthorized code that had been added to the code used by Annex Cloud to enable logins … and could have captured information entered during the checkout process by customers who placed or attempted to place orders on [Stein Mart's] website."

24. Stein Mart's letter acknowledged the very real threat that the Data Breach would result in fraudulent charges, identity theft, and other similar risks by further instructing Plaintiff Kyles to "closely review [her] payment card statements for any unauthorized charges":

> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the

> bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Information on additional steps you can take can be found on the following pages.
>
> We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we removed the Annex Cloud login feature from our website while the investigation is ongoing.

25. Although the letter was dated November 13, 2018, it stated that Stein Mart "sought additional information" from Annex "through October 25, 2018," which indicates that both Stein Mart and Annex were aware of the Data Breach at least three weeks prior to sending letters to consumers informing them of its occurrence.

26. Moreover, the Vermont Office of Attorney General's website contains a letter dated September 14, 2018, from Stein Mart that is nearly identical to the one sent to Plaintiff Kyles, which indicates that both Stein Mart and Annex were aware of the Data Breach at least as of September 14, 2018.

27. Had Plaintiff Kyles known that Defendants would not adequately protect the Personal Information and other sensitive information entrusted to them, she would not have transmitted her Personal Information to Defendants and/or allowed Defendants to store her Personal Information.

28. As a result of Defendants' failure to adequately safeguard Plaintiff Kyles' Personal Information, Plaintiff Kyles has been injured.

Defendant Stein Mart

29. Stein Mart describes itself as a national specialty retailer offering designer and name-brand fashion apparel at discounted prices.

30. Stein Mart is incorporated in Florida, and its headquarters is located at 1200 Riverplace Boulevard, Jacksonville, Florida 33207-9046.

Defendant Annex

31. Annex describes itself as a company that serves as a third-party vendor for online merchants/retailers (such as Stein Mart) and offers a service through which consumers can use their accounts with websites such as Facebook and Amazon to log into internet merchants'/retailers' websites to make online purchases.

32. Annex is incorporated in Delaware, and its headquarters is located at 5301 Beethoven Street, Suite 134, Los Angeles, California 90066.

JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A).

34. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

35. This Court has personal jurisdiction over Defendants because, inter alia, they have sufficient minimum contacts with the state of Delaware and intentionally avail themselves of the consumers and markets within the state through the promotion, marketing, and sale of their products and services. Furthermore, this Court has personal jurisdiction over Annex because it is incorporated in Delaware.

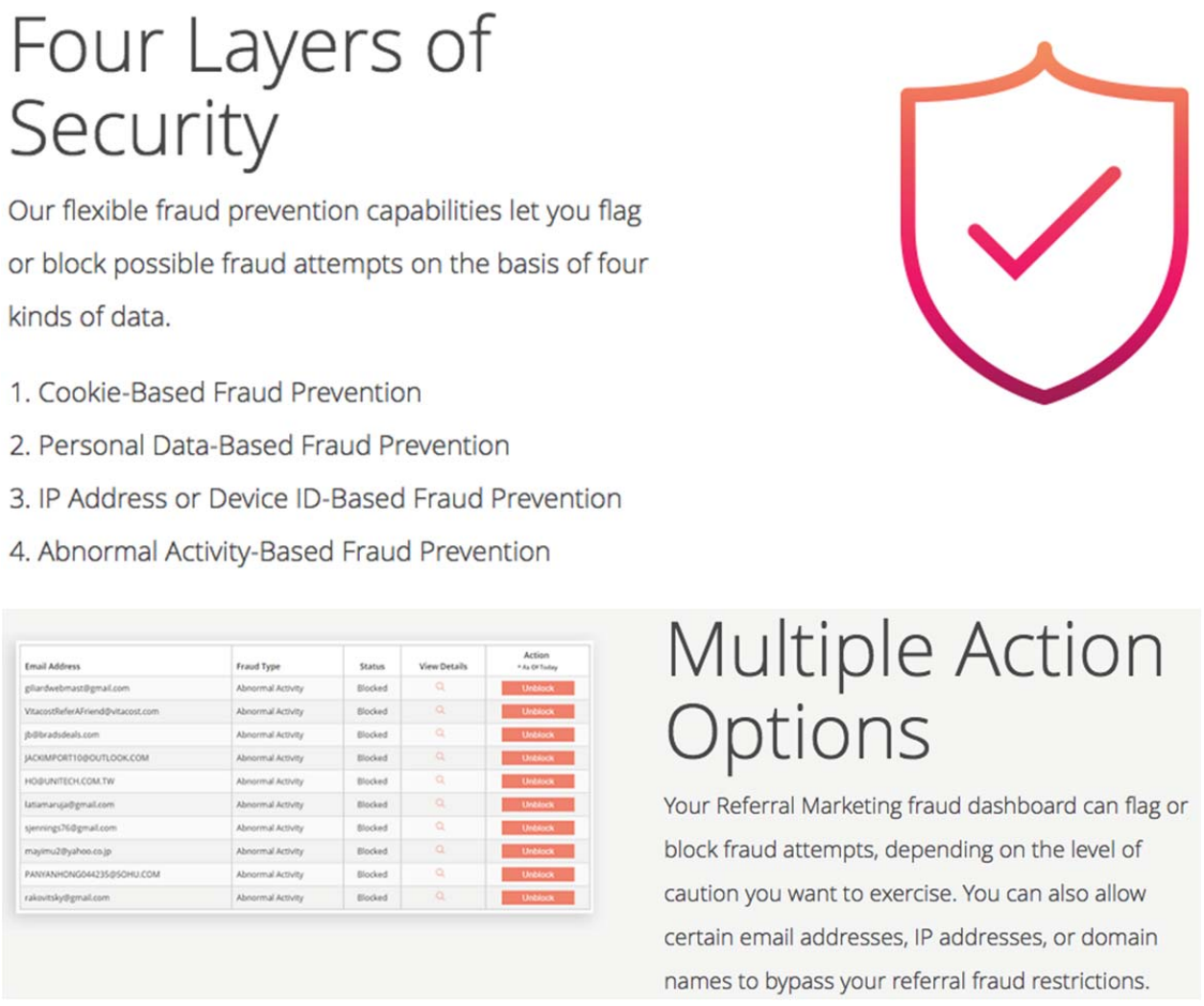
36. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because, *inter alia,* Annex is incorporated in Delaware and both Defendants conduct substantial business in this district. A substantial part of the events and/or omissions giving rise to the claims occurred, in part, within this district.

FACTUAL ALLEGATIONS

Annex's Safety and Privacy Guarantees to Consumers

37. Annex's website[1] contains an entire page devoted to "Fraud Prevention," with a header: "Secure Referrals: Keeping Your Bottom Line Safe," which states: "Our four-layered security protocol protects you in the case of any event."

38. Annex's website contains the following pages about maintaining data security and safety entrusted to it:



[1] Accessible at: https://www.annexcloud.com/referral-marketing-fraud-prevention (last visited: March 8, 2019).

39. Despite the foregoing assurances, however, Annex failed to adequately protect Plaintiffs' and class members' (defined below) Personal Information.

Stein Mart's Safety and Privacy Guarantees to Consumers

40. Similar to Annex's representations above from its website, Stein Mart's website[2] also "guarantees" customers that it will protect their sensitive Personal Information, including their payment card information:

Secure Shopping Guarantee

We use the industry standard encryption protocol known as Secure Socket Layer (SSL) to keep your order information secure.

We have established a Secure Shopping Guarantee with Norton Security for every transaction that you make with Steinmart.com. Should any unauthorized charges appear on your credit card as a result of shopping with Steinmart.com, you must notify your credit card provider in accordance with its reporting rules and procedures.

You should always see the Norton Shopping Guarantee seal with today's date displayed in the lower corner of the cart and checkout pages.

The Norton Shopping Guarantee provides:

1. $10,000 Identity Theft Protection - Receive comprehensive assistance and financial coverage if your identity is stolen anywhere online or offline.
2. $1,000 Purchase Guarantee - All terms (returns, refunds, shipping, etc.) are independently guaranteed.
3. $100 Lowest Price Guarantee - If the published store price drops, we will pay you the difference, up to $100.
4. Benefits, Terms and Conditions of the Norton Shopping Gaurantee

41. Despite the foregoing guarantees, however, Stein Mart failed to adequately protect Plaintiffs' and class members' (defined below) Personal Information.

The Data Breach

42. On September 14, 2018, Stein Mart filed with the Vermont Attorney General a notice of the Data Breach that mirrored the language of the letters sent to individual consumers (including Plaintiffs) two months later notifying them of the Data Breach.

[2] Accessible at: https://www.steinmart.com/category/customer+service/privacy+and+security.do (last visited: March 8, 2019).

43. As discussed above, the notice explained that Annex is a company that provides a service used by websites that enable consumers to use their user name and password from other websites—such as Facebook and Amazon—to log in to internet merchants' websites, such as Stein Mart's website, to make online purchases thereon, and that Annex's system was accessed by unauthorized users who were able to capture customers'/consumers' Personal Information, including payment card information, entered on Stein Mart's website while making online purchases.

44. Specifically, the Notice states "Annex Cloud informed Stein Mart that they had detected and removed unauthorized code that had been added to the code used by Annex Cloud to enable logins … and could have captured information entered during the checkout process by customers who placed or attempted to place orders on [Stein Mart's] website [on]: May 19, June 1, June 7 … including card number, expiration date, and card security code (CVV)."

45. Stein Mart's letter acknowledged the very real threat that the Data Breach would result in fraudulent charges, identity theft, and other similar risks by further instructing recipients of the letter—such as Plaintiffs—to "closely review [their] payment card statements for any unauthorized charges":

> We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. Information on additional steps you can take can be found on the following pages.
>
> We regret that this incident occurred and apologize for any inconvenience. To help prevent a similar incident from occurring in the future, we removed the Annex Cloud login feature from our website while the investigation is ongoing.

46. Stein Mart's subsequent letters sent to individual customers two months after the Vermont letter stated that the Data Breach was more widespread than originally reported because

Annex Cloud identified additional periods of time during which customers' Personal Information may have been captured by unauthorized users from December 28, 2017 through at least July 9, 2018.

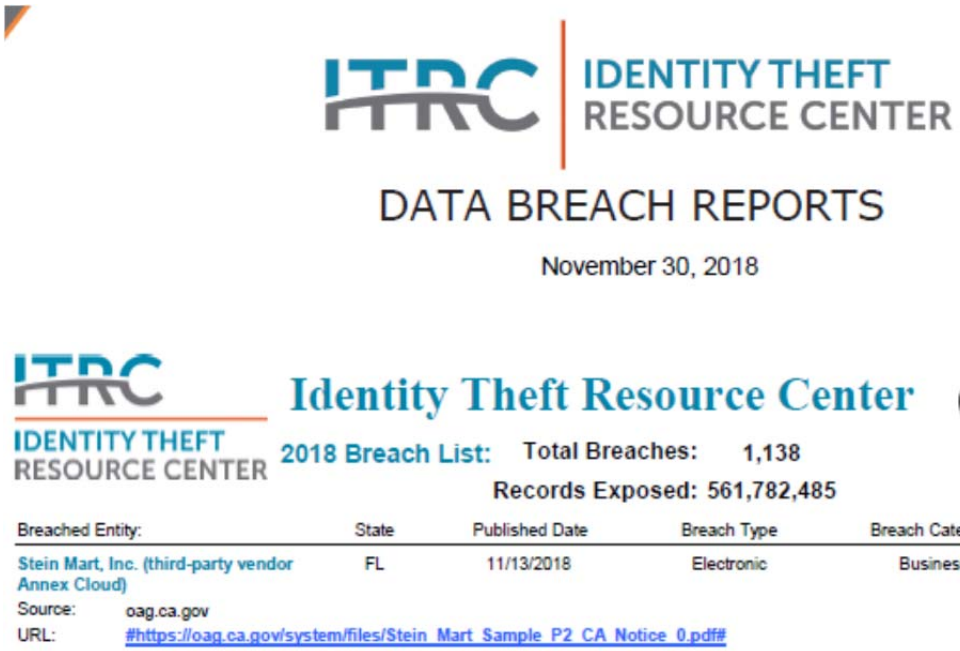
47. Thus, it was not until nearly eleven months after the initial breach that Defendants notified individuals affected by the Data Breach.

48. Notably, neither Stein Mart nor Annex offered customers free credit monitoring. Instead, they merely provided customers with contact information for Equifax, Experian, and Transunion, as well as for the Federal Trade Commission-Consumer Response Center. Both Defendants made general suggestions to contact local authorities and police, in addition to suggestions on implementing a credit freeze if necessary. Essentially, all of these steps are mandated generalities used by virtually every company when publishing alerts about data security breaches; neither Defendant made any additional effort to mitigate or remediate the damage caused by the Data Breach.

49. On November 7, 2018, Stein Mart filed a notice of the Data Breach with the California Attorney General that identified additional dates that the Data Breach occurred above those reported in Stein Mart's original communications to affected customers. Specifically, the California Notice stated that the time period during which the Data Breach occurred includes any date between December 28, 2017 and July 9, 2018.

50. Additionally, as of latest update from Annex Cloud on October 25, 2018, there are certain periods of time within this range of dates where it is not clear if unauthorized code used by hackers was present or not.

51. A report from the Identity Theft Resource Center ("ITRC") dated November 30, 2018, titled "Data Breach Reports" provides that the number of individuals affected by the Data Breach remains unknown as of the date of that report[3]:



ITRC | IDENTITY THEFT RESOURCE CENTER

DATA BREACH REPORTS

November 30, 2018

ITRC IDENTITY THEFT RESOURCE CENTER — Identity Theft Resource Center — CYBER SCOUT

2018 Breach List: Total Breaches: 1,138

Records Exposed: 561,782,485

Breached Entity:	State	Published Date	Breach Type	Breach Category	Records Reported
Stein Mart, Inc. (third-party vendor Annex Cloud)	FL	11/13/2018	Electronic	Business	Unknown

Source: oag.ca.gov

URL: #https://oag.ca.gov/system/files/Stein_Mart_Sample_P2_CA_Notice_0.pdf#

52. Notably, other online retailers were affected by the same breach of Annex Cloud include, but are not necessarily limited to, Francesca's Services Corporation, Title Nine, DiscountMugs.com, and SHEIN.

53. Numerous online news stories were published reporting the facts of the Data Breach. For instance, *ZD Net.com* published a story on September 24, 2018[4] titled, "SHEIN Fashion Retailer Announces Breach Affecting 6.42 Million Users," which provided that SHEIN, another online fashion store, announced that approximately 6.42 million of its customers were

[3] https://www.idtheftcenter.org/wp-content/uploads/2018/12/2018-November-Data-Breach-Package.pdf (last visited Feb. 12, 2019).

[4] https://www.zdnet.com/article/shein-fashion-retailer-announces-breach-affecting-6-42-million-users/ (last visited February 12, 2019).

potentially affected by the Annex Cloud Breach. SHEIN announced that it hired a forensic cybersecurity firm and international law firm to investigate the breach.

54. Based on the foregoing—and upon information and belief—Plaintiff and the Class' Personal Information was stolen, acquired, accessed, downloaded, and/or viewed by unauthorized persons from Defendants' websites or systems.

55. Furthermore, as stated in its letter, Stein Mart withheld disclosure of the Breach from Plaintiffs and the Class for at least two months, and did not notify customers of it until at least eleven months after it occurred.

56. Neither the statement on Defendants' website, nor the contemporaneous statements by Defendants to media outlets gave any indication as to the magnitude of the Data Breach or the number of customers affected. However, upon information and belief, the Data Breach affected the large majority of individuals who are customers and, in turn, users of Defendants' various business services.

57. Defendants' own public statements confirm that the Breach will subject Plaintiffs and the Class to continued, future risk of identity theft, fraudulent charges and other damages. For instance, Defendants stated to consumers "We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported."

Industry Standards and the Protection of Customer Personal Information

58. It is well known that customer Personal Information is valuable and frequently targeted by hackers. Despite the risk of a data breach and the widespread publicity and industry

alerts regarding the other notable data breaches, Defendants failed to take reasonable steps to adequately protect their computer systems from being breached.

59. Defendants are, and at all relevant times have been, aware that the Personal Information they maintain is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

60. As reflected in the screenshots above from Stein Mart's and Annex's websites, Defendants' various website pages acknowledge that their customers/clients expect them to adequately safeguard their customers' Personal Information.

61. Defendants are, and at all relevant times have been, aware of the importance of safeguarding customers' Personal Information and of the foreseeable consequences that would occur if their data security systems were breached.

62. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

63. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

64. 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 network's 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.

65. The FTC has also 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.[5]

66. Furthermore, the Payment Card Industry Data Security Standard ("PCI DSS") is promulgated by the Payment Card Industry Security Standards Council, and consists of twelve actionable steps companies should take to secure data information. The twelve steps of the PCI DSS are:

(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;

(3) Protect stored cardholder data;

(4) Encrypt transmission of cardholder data across open, public networks;

(5) Protect all systems against malware and regularly update anti-virus software or programs;

(6) Develop and maintain secure systems and applications;

(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;

[5] FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personalinformation-guide-business_0.pdf.

(10) Track and monitor all access to network resources and cardholder data;

(11) Regularly test security systems and processes;

(12) Maintain a policy that addresses information security for all personnel.

67. Defendants knew of these standards through their participation in the payment card processing networks.

68. As noted above, Defendants should have been aware of the need to have adequate data security systems in place.

69. Despite this, Defendants failed to upgrade and maintain their data security systems in a meaningful way so as to prevent data breaches. Had Defendants maintained their information technology ("IT") systems and adequately protected them, they could have prevented the Data Breach.

70. As a result of industry warnings, industry practice, and multiple well-documented data breaches, Defendants were alerted to, and in turn aware of, the risks associated with failing to ensure that their IT systems were adequately secured.

71. Defendants were not only aware of the threat of data breaches, generally, but were aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Defendants were aware that malware is a real threat and is a primary tool of infiltration used by hackers.

72. In addition to the publicly announced data breaches described above, Defendants received additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted

retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[6]

73. Despite the fact that Defendants were on notice of the very real possibility of consumer data theft associated with their security practices and that Defendants knew or should have known about the elementary infirmities associated with their security systems, they still failed to make necessary changes to its security practices and protocols.

74. Defendants, at all times relevant to this action, had a duty to Plaintiffs and members of the Class to: (a) properly secure Personal Information submitted to or collected on Defendants' websites and on Defendants' internal networks; (b) encrypt Personal Information using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the Class, which would naturally result from Personal Information theft; and (e) promptly notify customers when Defendants became aware of the potential that customers' Personal Information may have been compromised.

75. Defendants negligently allowed Personal Information to be compromised by failing to take reasonable steps against an obvious threat.

76. In addition, leading up to the Data Breach, and during the course of the breach itself and the investigation that followed, Defendants failed to follow the guidelines set forth by the FTC.

77. As a result of the events detailed herein, Plaintiffs and members of the Class suffered losses resulting from the Data Breach, including loss of time and money resolving

[6] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.

fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Stein Mart and/or through the use of Annex's services that Plaintiffs and Class members would not have made had they known of Defendants' careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

78. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

79. The information stolen from Defendants' websites can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

80. Even if credit card companies may be responsible for or reimburse some of the unauthorized transactions, consumers affected by the Data Breach may be liable for fraudulent charges below a threshold amount.

81. To date, Defendants do not appear to be taking any measures to assist affected customers other than telling them to simply do the following:

- "closely review your payment card statements for any unauthorized charges";
- "immediately report any such [unauthorized] charges to the bank that issued your card";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a credit freeze; and
- create a fraud alert.

None of these recommendations, however, require Defendants to expend any effort to protect Plaintiffs' and Class Members' Personal Information.

82. Defendants' failure to adequately protect consumers' Personal Information has resulted in consumers having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money—while Defendants sit by and do nothing to assist those affected by the Data Breach. Instead, as Stein Mart's letters indicate, Defendants are putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

83. Plaintiffs bring this action on their own behalf, and on behalf of the following Class pursuant to FED. R. CIV. P. 23:

> **Nationwide Class**
>
> All persons whose Personal Information was compromised by the data breach involving Annex Cloud at various times between December 28, 2017 and July 9, 2018. The class includes, without limitation, all customers of all website vendors (such as Stein Mart) which enabled class members' Personal Information to be compromised in the data breach. Plaintiffs reserve the right to amend the class definition and add additional vendors as parties.

84. The above class is referred to as the "Class." Excluded from the Class are Defendants, their affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change, or expand the definition of the Class based on discovery and further investigation.

85. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many thousands of members who are geographically

dispersed. Upon information and belief, the Data Breach affected people across the United States.

86. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their data and Personal Information compromised in the same way by the same conduct by Defendants.

87. **Adequacy**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in class action litigation; and Plaintiffs and their counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

88. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class-action device

presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

89. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiffs and all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether Defendants engaged in the wrongful conduct alleged herein;
- whether Defendants owed a duty to Plaintiffs and members of the Class to adequately protect their Personal Information and to provide timely and accurate notice of the breach to Plaintiffs and the Class, and whether they breached these duties;
- whether Defendants violated federal and state laws—including but not limited to state consumer protection laws and data privacy laws (e.g., Section 5 of the FTC Act, 15 U.S.C. § 45; South Carolina's Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*; the Missouri Merchandising Practices Act, MO. ANN. STAT. § 407.020(1), *et seq.*) thereby breaching their duties to Plaintiffs and the Class;
- whether Defendants knew or should have known that their computer and network systems were vulnerable to attack from hackers;
- whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach of their computer and network systems resulting in the loss of consumers' Personal Information;
- whether Defendants wrongfully failed to inform Plaintiffs and members of the Class that they did not maintain computer software and other security procedures sufficient to reasonably safeguard highly-sensitive personal data;
- whether Defendants failed to inform Plaintiffs and the Class of the data breach in a timely and accurate manner;
- whether Defendants wrongfully waited to inform Plaintiffs and Class members that their sensitive Personal Information was exposed in the security breach;
- whether Defendants continue to breach duties to Plaintiffs and Class;
- whether Defendants have sufficiently addressed, remedied, or protected Plaintiffs and Class members following the data breach and have taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;

- whether Plaintiffs and members of the Class suffered injury as a proximate result of Defendants' conduct or failure to act; and

- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

90. Defendants have acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

91. Given that Defendants have engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved and common questions far outweigh any potential individual questions.

92. The Class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Personal Information to cyber criminals due to Defendants' failure to protect this information and adequately warn the Class that it was breached. Class membership will be readily ascertainable from Defendants' business records.

93. Plaintiffs reserve the right to revise the above Class definition based on facts adduced in discovery.

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

94. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

95. Defendants obtained sensitive Personal Information from Plaintiffs and Class members in their provision of online retail transactions and Annex's services provided to Stein Mart to facilitate those transactions.

96. Defendants owed a duty to Plaintiffs and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their Personal Information in Defendants' possession from being compromised by unauthorized persons. This duty included, *inter alia*, designing, maintaining, and testing Defendants' security systems to ensure that Plaintiffs' and Class members' Personal Information was adequately protected both in the process of collection and after collection.

97. Defendants further owed a duty to Plaintiffs and Class members to implement processes that would detect a breach of their security system in a timely manner and to timely act upon warnings and alerts.

98. Defendants owed a duty to Plaintiffs and Class members to provide security consistent with industry standards and requirements and to ensure that their computer systems and networks—and the personnel responsible for them—adequately protected the Personal Information of Plaintiffs and Class members whose confidential data Defendants obtained and maintained.

99. Defendants hold themselves out as experts in legal compliance, and thus knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiffs and Class members and of the critical importance of providing adequate security for that information.

100. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and members of the Class. This conduct included but was not limited to Defendants' failure to take the steps and opportunities to prevent and stop the Data Breach as described above. Defendants' conduct also included their decisions not to comply with industry standards for the safekeeping and maintenance of Plaintiffs' and Class members' Personal Information.

101. Defendants knew or should have known that they had inadequate computer systems and data security practices to safeguard such information, and Defendants knew or should have known that hackers were attempting to access the Personal Information in databases such as Defendants'.

102. Defendants breached the duties they owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiffs and members of the Class, as identified above. This Data Breach was a proximate cause of injuries and damages suffered by Plaintiffs and Class members.

103. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered harm to their personal property by way of their sensitive Personal Information—including but not limited to, their payment cards, credit profiles, credit card balances, and bank accounts—being altered, depleted, reduced, compromised and/or accessible by unauthorized users. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have also suffered the loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Stein Mart and/or through the use of Annex's services that Plaintiffs and Class members would not have made had they known of Defendants' careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information, entitling them to damages in an amount to be proven at trial.

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

104. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

105. Pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45 (among the other state consumer data privacy laws), Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Personal Information.

106. 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 Defendants, of failing to use reasonable measures to protect Card Information. The FTC publications and orders described above also form part of the basis of Defendants' duty.

107. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Personal Information they collected and stored—which included highly sensitive payment card data—and the foreseeable consequences of a breach, including, specifically, the immense damages that would result to consumers.

108. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, 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.

109. Defendants had a duty to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' Personal Information.

110. Defendants breached their duties to Plaintiffs and Class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate data security practices to safeguard Plaintiffs' and Class members' Personal Information.

111. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

112. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class members, Plaintiffs and Class members would not have been injured.

113. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known they were failing to meet their duties and that their breaches would cause Plaintiffs and Class members to suffer the foreseeable harm associated with the exposure of their sensitive Personal Information.

114. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered harm to their personal property by way of their sensitive Personal Information—including but not limited to, their payment cards, credit profiles, credit card balances, and bank accounts—being altered, depleted, reduced, compromised and/or accessible by unauthorized users. As a direct and proximate result of Defendants' negligence *per* se, Plaintiffs and Class Members have also suffered the loss of time and money resolving fraudulent

charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Stein Mart and/or through the use of Annex's services that Plaintiffs and Class members would not have made had they known of Defendants' careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

115. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

116. Plaintiffs and Class members whose Personal Information is obtained by Defendants in connection with their provision of online retail and payment services have valid, binding, and enforceable implied contracts with Defendants.

117. Specifically, Plaintiffs and Class members agreed to the release of their sensitive Personal Information to Defendants to be used in connection with their provision of online retail and payment services. In exchange, Defendants agreed, among other things: (1) to provide online retail and payment services to Plaintiffs and Class members; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' Personal Information; and (3) to protect Plaintiffs' and Class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

118. Protection of Personal Information is a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Defendants, on the other hand. Plaintiffs and Class members consented—implicitly or explicitly—to the release of their sensitive Personal Information to Defendants. Had Plaintiffs and Class members known that Defendants would not adequately protect their Personal Information, they would not have consented to their Personal Information being provided to Defendants.

119. Defendants did not satisfy their promises and obligations to Plaintiffs and Class members under the implied contracts because they did not take reasonable measures to keep Plaintiffs' and Class members' Personal Information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

120. Defendants materially breached their implied contracts with Plaintiffs and Class members by failing to implement adequate data security measures.

121. Plaintiffs and Class members fully performed their obligations under their implied contracts with Defendants.

122. Defendants' failure to satisfy their obligations led directly to the successful intrusion of Defendants' computer servers and stored Personal Information and led directly to unauthorized parties' access and exfiltration of Plaintiffs' and Class members' sensitive Personal Information.

123. Defendants breached these implied contracts as a result of its failure to implement adequate data security measures.

124. Also, as a result of Defendants' failure to implement the security measures, Plaintiffs and Class members have suffered actual damages resulting from the theft of their Personal Information and remain at imminent risk of suffering additional damages in the future.

125. Accordingly, Plaintiffs and Class members have been injured as a proximate result of Defendants' breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

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

126. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

127. This claim is plead in the alternative to the above contract claim.

128. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for the purchase of products from Stein Mart's website, which were processed or otherwise facilitated using Annex's services.

129. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class Members. Defendants also benefited from the receipt of Plaintiffs' and Class members' Card Information, which was utilized by Defendants to facilitate payment to Stein Mart using Annex's services (for which Annex was compensated by Stein Mart).

130. The monies for products that Plaintiffs and Class Members paid to Stein Mart, by way of Annex's services (for which Annex was compensated from Stein Mart), were supposed to be used by both Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

131. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between products and services offered with the reasonable data privacy and security practices and procedures that Plaintiffs and Class

Members paid for and the inadequate products and services without reasonable data privacy and security practices and procedures that they received.

132. Under principals of equity and public policy, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws, as well as industry standards and public policy.

133. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class Members all unlawful or inequitable proceeds received by them as a result of the conduct and data breach alleged herein.

COUNT V
Violation of the Missouri Merchandising Practices Act
MO. ANN. STAT. § 407.020(1), et seq. ("MMPA")
(By Plaintiff Ande Kyles Individually and on Behalf of the Class)

134. Plaintiff Kyles incorporates all foregoing substantive allegations as if fully set forth herein.

135. This claim is brought on behalf of Plaintiff Kyles and the Class.

136. The MMPA provides in part:

> The act, … by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce … is declared to be an unlawful practice.

MO. ANN. STAT. § 407.020.

137. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Personal Information of Plaintiff Kyles and the Class, Defendants violated the provisions of § 407.020 of the MMPA.

138. Defendants' actions as set forth above occurred in the conduct of trade or commerce.

139. The acts and conduct of Defendants as alleged above violated the MMPA by, among other things:

- failing to maintain sufficient security to keep confidential and sensitive financial information of Plaintiff Kyles and the Class from being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of goods and providing online purchases services, by representing that Defendants would maintain adequate data privacy and security practices and procedures to safeguard Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with the sale of goods and providing online purchases services, by representing that Defendants did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members' personal information; and,
- failing to prevent the Data Breach and promptly notify consumers thereof, failing to maintain the privacy and security of Class members' personal information, in violation of duties imposed by and public policies reflected in applicable federal and state laws.

140. Due to the Data Breach, Plaintiff Kyles and the Class have lost property in the form of their Personal Information and have suffered actual damages. Further, Defendants' failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Plaintiff Kyles and the Class spending time and money to protect against identity theft. Plaintiff Kyles and the Class are now at a higher risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendants' practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

141. As a result of Defendants' practices, Plaintiff Kyles and the Class have suffered injury-in-fact and have lost money or property. As a result of Defendants' failure to adopt,

implement, and maintain reasonable security procedures, and the resulting Data Breach, Plaintiff Kyles and members of the Class have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

COUNT VI
Violation of the South Carolina's Unfair Trade Practices Act
S.C. Code Ann. § 39-5-20(a), *et seq*. ("SCUTPA")
(By Plaintiff Diane Taylor Individually and on Behalf of the Class)

142. Plaintiff Taylor incorporates all foregoing substantive allegations as if fully set forth herein.

143. Defendants engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of goods or services to consumers, including Plaintiff Taylor and Class Members.

144. Defendants are engaged in, and their acts and omissions affect, trade and commerce. Defendants' acts, practices and omissions were done in the course of their business of marketing, offering for sale and selling goods and services throughout the United States, including in Delaware.

145. Defendants' conduct as alleged in this Complaint, including without limitation, their failure to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information, Defendants' failure to disclose the material fact that their computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, Defendants' failure to disclose in a timely and accurate manner to Plaintiff Taylor and Class Members the material fact of the Data Breach, and Defendants' continued acceptance of Plaintiff Taylor's and Class members' credit and debit card payments for purchases at Stein Mart after Defendants knew or should have known of the Data

Breach constitutes unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices.

146. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and concealment, suppression, and omission of material facts in connection with the sale of consumer goods in violation of the SCUTPA. Defendants' acts and practices are unfair and/or deceptive in at least the following respects:

- failing to maintain sufficient security to keep Plaintiff Taylor's and Class Members' sensitive Personal Information being hacked and stolen;
- misrepresenting material facts to the Class, in connection with the sale of products, by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Personal Information from unauthorized disclosure, release, data breaches, and theft;
- misrepresenting material facts to the Class, in connection with sale of products, by representing that Defendants did and would (or omitting that they would not) comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' Personal Information; and
- failing to take proper action following the data breach to enact adequate privacy and security measures and protect Class Members' Personal Information and other personal information from further unauthorized disclosure, release, data breaches, and theft.

147. In addition, Defendants' failure to disclose that their computer systems were not well-protected and that Plaintiff Taylor's and Class members' sensitive Personal Information was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendants knew such facts would (a) be unknown to and not easily discoverable by Plaintiff Taylor and the Class; and (b) defeat Plaintiff Taylor's and Class Members' ordinary, foreseeable, and reasonable expectations concerning the security of their Personal Information on Defendants' computer servers.

148. Defendants intended that Plaintiff Taylor and Class Members would rely on their deceptive and unfair acts and practices, misrepresentations, and concealment, suppression, and

omission of material facts in connection with their offering of products and incorporating Plaintiff Taylor's and Class Members' Personal Information on its computer servers in violation of the SCUTPA.

149. Defendants also engaged in unfair acts and practices in connection with the provision of payment services by failing to maintain the privacy and security of Class Members' Personal Information in violation of duties imposed by and public policies reflected in applicable federal and state laws resulting in the Data Breach.

150. Defendants' acts and practices are contrary to South Carolina law and policy and constitute immoral, unethical, oppressive, and unscrupulous business practices that caused substantial injury to—and had the tendency to deceive—Plaintiff Taylor and Class Members. The gravity of the harm resulting from Defendants' unfair conduct outweighs any potential utility of the conduct.

151. Defendants' wrongful practices were and are injurious to the public interest because those practices were part of a generalized, common, and uniform course of wrongful conduct on the part of Defendants that applied to all Class Members and were repeated continuously before and after Defendants obtained sensitive Personal Information and other information from Plaintiff Taylor and Class Members.

152. Defendants' wrongful practices had an adverse impact on the public and the potential for repetition because data breaches such as the Data Breach alleged herein have occurred in the past and will thus likely continue to occur in the future absent deterrence, and Defendants' procedures (i.e., their failure to adequately safeguard Plaintiff Taylor's and Class Members' Personal Information) create the potential for repetition in the future.

153. All Class members and Plaintiff Taylor could not reasonably avoid the harm from Defendants' unfair conduct.

154. As a result of Defendants' wrongful conduct, Plaintiff Taylor and Class Members were injured in that they would not have allowed their sensitive Personal Information—the value of which Plaintiff Taylor and Class Members no longer have control—to be provided to Defendants if they had been told or knew that Defendants failed to maintain sufficient security to keep such data from being hacked and taken by others.

155. Defendants' unfair and/or deceptive conduct proximately caused Plaintiff Taylor's and Class Members' injuries because, had Defendants maintained customer Personal Information with adequate security, Plaintiff Taylor and the Class Members would not have lost it.

156. As a direct and proximate result of Defendants' conduct, Plaintiff Taylor and Class Members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Stein Mart that Plaintiff Taylor and Class Members would have never made had they known of Defendants' careless approach to cybersecurity; lost control over the value of Personal Information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Personal Information entitling them to damages in an amount to be proven at trial.

157. Defendants acted with willful and conscious disregard of the rights of others, subjecting Plaintiff Taylor and Class Members to unjust hardship as a result such that an award of punitive damages is appropriate.

158. Plaintiff Taylor and the Class seek actual damages, compensatory, punitive damages, injunctive relief, and court costs and attorneys' fees as a result of Defendants' violations of the SCUTPA.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Dated: March 8, 2019

Respectfully submitted,

/s/ Tiffany J. Cramer

Robert J. Kriner, Jr. (Del. Bar. No. 2546)
Scott M. Tucker (Del. Bar. No. 4925)
Tiffany J. Cramer (Del. Bar No. 4998)
Vera G. Belger (Del. Bar. No. 5676)
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
2711 Centerville Rd, Ste. 201
Wilmington, DE 19808
(302) 656-2500
rjk@chimicles.com
smt@chimicles.com
tjc@chimicles.com
vgb@chimicles.com

Benjamin F. Johns
Mark B. DeSanto
CHIMICLES SCHWARTZ KRINER
& DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
mbd@chimicles.com

Cornelius P. Dukelow
Oklahoma Bar No. 19086
Abington Cole + Ellery
320 South Boston Avenue, Suite 1130
Tulsa, Oklahoma 74103
918.588.3400 (*telephone & facsimile*)
cdukelow@abingtonlaw.com
www.abingtonlaw.com

Counsel for Plaintiffs and the Putative Class

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

Ande Kyles and Diane Taylor

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

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

Robert J. Kriner, Jr., Scott M. Tucker, Tiffany J. Cramer, Vera G. Belger
Chimicles Schwartz Kriner & Donaldson-Smith LLP
2711 Centerville Rd, Ste 201, Wilmington, DE 19808; (302) 656-2500

DEFENDANTS

Stein Mart, Inc. and Social Annex, Inc. (d/b/a Annex Cloud)

County of Residence of First Listed Defendant
(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)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	**PERSONAL INJURY**	**PERSONAL INJURY**	☐ 625 Drug Related Seizure of Property 21 USC 881	☐ 422 Appeal 28 USC 158	☐ 375 False Claims Act
☐ 120 Marine	☐ 310 Airplane	☐ 365 Personal Injury - Product Liability	☐ 690 Other	☐ 423 Withdrawal 28 USC 157	☐ 376 Qui Tam (31 USC 3729(a))
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		**PROPERTY RIGHTS**	☐ 400 State Reapportionment
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability		☐ 820 Copyrights	☐ 410 Antitrust
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	**PERSONAL PROPERTY**	**LABOR**	☐ 830 Patent	☐ 430 Banks and Banking
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 710 Fair Labor Standards Act	☐ 835 Patent - Abbreviated New Drug Application	☐ 450 Commerce
☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 720 Labor/Management Relations	☐ 840 Trademark	☐ 460 Deportation
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 740 Railway Labor Act	**SOCIAL SECURITY**	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	☐ 751 Family and Medical Leave Act	☐ 861 HIA (1395ff)	☐ 480 Consumer Credit
☐ 190 Other Contract	☒ 360 Other Personal Injury		☐ 790 Other Labor Litigation	☐ 862 Black Lung (923)	☐ 490 Cable/Sat TV
☐ 195 Contract Product Liability	☐ 362 Personal Injury - Medical Malpractice		☐ 791 Employee Retirement Income Security Act	☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
☐ 196 Franchise				☐ 864 SSID Title XVI	☐ 890 Other Statutory Actions
				☐ 865 RSI (405(g))	☐ 891 Agricultural Acts
					☐ 893 Environmental Matters
					☐ 895 Freedom of Information Act
REAL PROPERTY	**CIVIL RIGHTS**	**PRISONER PETITIONS**	**IMMIGRATION**	**FEDERAL TAX SUITS**	☐ 896 Arbitration
☐ 210 Land Condemnation	☐ 440 Other Civil Rights	**Habeas Corpus:**	☐ 462 Naturalization Application	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
☐ 220 Foreclosure	☐ 441 Voting	☐ 463 Alien Detainee	☐ 465 Other Immigration Actions	☐ 871 IRS—Third Party 26 USC 7609	☐ 950 Constitutionality of State Statutes
☐ 230 Rent Lease & Ejectment	☐ 442 Employment	☐ 510 Motions to Vacate Sentence			
☐ 240 Torts to Land	☐ 443 Housing/ Accommodations	☐ 530 General			
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 535 Death Penalty			
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	**Other:**			
	☐ 448 Education	☐ 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)***:
Class Action Fairness Act 28 U.S.C. Section 1332(d)(2)

Brief description of cause:
Consumer Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE
03/08/2019

SIGNATURE OF ATTORNEY OF RECORD
/s/ Tiffany J. Cramer

FOR OFFICE USE ONLY

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

ClassAction.org