BRADLEY/GROMBACHER LLP
Marcus J. Bradley, Esq (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Phone: (805) 270-7100
Email: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
NOTHERN DISTRICT OF CALIFORNIA

SILVIA CORTEZ, KAYLA DREVENAK, AMANDA EDWARDS, SUSAN FERRYMAN, TAYLOR GROSE, KATHERINE HULSEY, SANDRA HUNDLEY, DEE R. IGLEHART, AMY JENKINS, STORMY LINGER, CRYSTAL LINGER, JUSTIN MIEIR, LISA MIKEC, BRIAN O'CONNOR, KELLY ROGERS, LOUSHANDRA VAUGHN, and BRITTNEY WOOD, individually, and on behalf of all others similarly situated,

Plaintiffs,

v.

BLACKHAWK NETWORK, INC., dba BLACKHAWK ENGAGEMENT SOLUTIONS,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Silvia Cortez, Kayla Drevenak, Amanda Edwards, Susan Ferryman, Taylor Grose, Katherine Hulsey, Sandra Hundley, Dee R. Iglehart, Amy Jenkins, Stormy Linger, Crystal Linger, Justin Mieir, Lisa Mikec, Brian O'Connor Kelly Rogers, Loushandra Vaughn, Brittney Wood, individually, and on behalf of all others similarly situated, bring this Class Action Complaint ("Complaint") against Defendant Blackhawk Network, Inc. d/b/a Engagement Solutions ("Blackhawk"" or "Defendant"), a California corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to his own actions, which are made on personal knowledge, the investigation of his counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Blackhawk Network, Inc., which offers branded payment programs, including prepaid gift cards, to customers.
2. Blackhawk Network, Inc. is headquartered in Pleasanton, California.
3. Blackhawk acts as a third-party service provider on behalf of Pathward N.A. ("Pathward"). Pathward uses Blackhawk to activate and manage certain prepaid cards referred to as Pathward Prepaid Cards ("Prepaid Card" or "Prepaid Cards").
4. Blackhawk operates the website https://www.MyPrepaidCenter.com ("MyPrepaidCenter.com") on behalf of Prepaid Card holders to activate and manage Pathward issued Prepaid Cards. To activate and use Prepaid Cards, Plaintiffs and Class Members were required to provide certain sensitive, non-public information to Defendant by entering their information on MyPrepaidCenter.com.
5. Unfortunately, Blackhawk failed to properly secure and safeguard the personally identifiable information provided by customers, including Plaintiffs and Class Members, that appeared on the MyPrepaidCenter.com profile, including, without limitation, their unencrypted and unredacted first and last names, email addresses, phone numbers ("PII"), their payment card data in combination with information "related to the Prepaid Card profiles," which included, but was not limited to, information added by customers to

PrepaidCenter.com, such as card numbers, expiration dates, and CVV security codes ("PCD") and other sensitive information (collectively with PII and PCD, "Private Information").[1]

6. On information and belief, this Data Breach was engineered and targeted at accessing and exfiltrating the Private Information of Plaintiffs and Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

7. Defendant's failure to prevent and detect the Data Breach is particularly egregious considering the nature of its business and the Private Information it collected, the myriad data breaches all over the country, and its own experience with a substantially similar data breach described in more detail below. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendant's customers provided Private Information, which can be used to commit fraud against Plaintiffs and Class Members as well as steal their identities.

8. Plaintiffs bring this class action against Blackhawk to seek damages for themselves and other similarly situated consumers impacted by the Data Breach ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiffs and other Class Members from further data breach incidents.

9. On or about October 31, 2022, Pathward[2] filed a Notice of Data Breach ("Notice") with the Attorneys General of several states. The Notice states, on September 11, 2022, Blackhawk "discovered irregular activity in connection" with MyPrepaidCenter.com.[3] Blackhawk claims it "took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022."[4] In addition, Blackhawk states the

[1] Blackhawk Network, *Notice of Data Breach* (Oct. 31, 2022), https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf.

[2] Pathward, N.A. is listed as the entity submitting the Notice of Data Breach on several Attorneys General's public data breach database, however the actual Notice of Data Breach is on Blackhawk Network letterhead and signed by Blackhawk's VP of Customer Service.

[3] *Ibid.*

[4] *Ibid.*

"unauthorized acquisition occurred between September 4-12, 2022."[5] The Notice provided to the Montana Attorney General, for example, is as follows:

> **What Happened?**
>
> On September 11, 2022, we discovered irregular activity in connection with www.MyPrepaidCenter.com, the website that Blackhawk operates for cardholders to activate and manage Pathward Prepaid Cards. We took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022. Our investigation revealed that the irregular activity involved unauthorized acquisition of information about you described below. The unauthorized acquisition occurred between September 4–12, 2022.
>
> **What Information Was Involved?**
>
> This incident involved information you provided for your www.MyPrepaidCenter.com profile, including your first and last name, email address, and phone number (if any). It also included information relating to your Pathward Prepaid Card(s) you added to your www.MyPrepaidCenter.com profile, such as card numbers, expiration dates, and CVV codes.

10. Also, on November 1, 2022, through its attorney Pathward filed an Additional Information Notice, presumably to serve as an addendum to the Notice, ("Addendum") with the Attorney General of Maine. The Addendum, dated September 11, 2022, states that "individuals who are receiving notification had useable Pathward Prepaid Cards impacted by this incident" and that "[i]ndividuals whose Non-Useable Cards were impacted by this incident are not receiving Notice."[6]

11. As a result of Defendant's failure to prevent the Data Breach, or detect it during its occurrence thousands of MyPrepaidCenter.com customers across the United States are suffering and will continue to suffer real and imminent harm as a direct consequence of Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to adequately audit and monitor its third party data security vendors; (d) failing to disclose to its customers the material fact that it

[5] *Ibid.*

[6] Kamran Salour, *Additional Information* (November 1, 2022) https://apps.web.maine.gov/online/aeviewer/ME/40/52a7dc3e-1734-4ea7-b1a8-6e8d49176588.shtml

or its vendors did not have adequate computer systems and security practices to safeguard customers' personal and financial information; and (e) failing to provide timely and adequate notice of the data breach.

12. The injuries suffered by Plaintiffs and Class Members as a direct result of the Data Breach include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The present and continuing injury flowing from potential theft, fraud, and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted to Blackhawk for the sole purpose of using Blackhawk's services and with the mutual understanding that Blackhawk would safeguard Plaintiffs' and Class Members' Private Information against theft and not allow access to and misuse of their information by others;

h. Money paid to Blackhawk during the period of the Data Breach in that Plaintiffs and Class Members would not have used Blackhawk's services or products, or would have paid less for their services or products, had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Private Information and had Plaintiffs and Class Members known that Blackhawk would not provide timely and accurate notice of the Data Breach; and,

i. Continued risk to their PII, which remains in the possession of Blackhawk and its vendors, and which is subject to further breaches so long as Blackhawk continues to fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data in its possession.

13. Examples of the harms experienced by Blackhawk customers as a direct and foreseeable consequence of its conduct include the experiences of the representative Plaintiffs described below.

II. THE PARTIES

Plaintiff Silvia Cortez

14. Plaintiff Silvia Cortez is a citizen of the State of Texas and a is a resident of Houston, Texas. Plaintiff Cortez had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Cortez had ten Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use those Prepaid Cards, Plaintiff Cortez was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Cortez reasonably expected that Defendant would safeguard her Private Information. Plaintiff Cortez would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Cortez has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

Plaintiff Kayla Drevenak

15. Plaintiff Kayla Drevenak is a citizen of the State of Pennsylvania and a is a resident of Wilkes Barre, Pennsylvania. Plaintiff Drevenak had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Drevenak had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Drevenak was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Drevenak reasonably expected that Defendant would safeguard her Private Information. Plaintiff Drevenak would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Drevenak has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Amanda Edwards

16. Plaintiff Kayla Edwards is a citizen of the State of Maine and a is a resident of Lisbon, Maine. Plaintiff Edwards had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Edwards had thirty Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff Edwards was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Edwards reasonably expected that Defendant would safeguard her Private Information. Plaintiff Edwards would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Edwards has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

/ / /

Plaintiff Susan Ferryman

17. Plaintiff Susan Ferryman is a citizen of the State of Ohio and a is a resident of Springfield, Ohio. Plaintiff Ferryman had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Ferryman had thirty Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff Ferryman was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Ferryman reasonably expected that Defendant would safeguard her Private Information. Plaintiff Ferryman would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Ferryman has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Taylor Grose

18. Plaintiff Taylor Grose is a citizen of the State of Montana and a is a resident of West Plains, Montana. Plaintiff Grose had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Grose had three Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff Grose was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Grose reasonably expected that Defendant would safeguard her Private Information. Plaintiff Grose would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Grose has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

/ / /

Plaintiff Katherine Hulsey

19. Plaintiff Katherine Hulsey is a citizen of the State of Montana and a is a resident of Lake Saint Louis, Montana. Plaintiff Hulsey had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Hulsey had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Hulsey was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Hulsey reasonably expected that Defendant would safeguard her Private Information. Plaintiff Hulsey would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Hulsey has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Sandra Hundley

20. Plaintiff Sandra Hundley is a citizen of the State of Ohio and a is a resident of Middletown, Ohio. Plaintiff Hundley had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Hundley had four Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff Hundley was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Hundley reasonably expected that Defendant would safeguard her Private Information. Plaintiff Hundley would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Hundley has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

/ / /

Plaintiff Dee R. Iglehart

21. Plaintiff Dee R. Iglehart is a citizen of the State of Illinois and a is a resident of Mt Carmel, Illinois. Plaintiff Iglehart had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Iglehart had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Iglehart was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Iglehart reasonably expected that Defendant would safeguard her Private Information. Plaintiff Iglehart would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Iglehart has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Amy Jenkins

22. Plaintiff Amy Jenkins is a citizen of the State of Virginia and a is a resident of Hopewell, Virginia. Plaintiff Jenkins had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Jenkins had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Jenkins was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Jenkins reasonably expected that Defendant would safeguard her Private Information. Plaintiff Jenkins would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Jenkins has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

/ / /

Plaintiff Stormy Linger

23. Plaintiff Stormy Linger is a citizen of the State of West Virginia and a is a resident of Buckhannon, West Virginia. Plaintiff Stormy Linger had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Stormy Linger had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Stormy Linger was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Stormy Linger reasonably expected that Defendant would safeguard her Private Information. Plaintiff Stormy Linger would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Stormy Linger has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Crystal Linger

24. Plaintiff Crystal Linger is a citizen of the State of West Virginia and a is a resident of Buckhannon, West Virginia. Plaintiff Crystal Linger had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Crystal Linger had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Crystal Linger was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Crystal Linger reasonably expected that Defendant would safeguard her Private Information. Plaintiff Crystal Linger would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Crystal Linger has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Justin Mieir

25. Plaintiff Justin Mieir is a citizen of the State of North Carolina and a is a resident of Henderson, North Carolina. Plaintiff Mieir had his Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Mieir had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Mieir was required to create an account on MyPrepaidCenter.com and provide Defendant with his Private Information. In making his decision to create an account to gain full access to his Prepaid Card, Plaintiff Mieir reasonably expected that Defendant would safeguard his Private Information. Plaintiff Mieir would not have created an account, nor would have provided Private Information, if he knew that the Private Information collected by Defendant would be at risk. Plaintiff Mieir has suffered damages and remains at a significant risk now that his Private Information has been leaked online.

Plaintiff Lisa Mikec

26. Plaintiff Lisa Mikec is a citizen of the State of Pennsylvania and a is a resident of Houston, Pennsylvania. Plaintiff Mikec had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Mikec had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Mikec was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Mikec reasonably expected that Defendant would safeguard her Private Information. Plaintiff Mikec would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Mikec has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

/ / /

/ / /

Plaintiff Brian O'Connor

27. Plaintiff Brian O'Connor is a citizen of the State of California and a is a resident of Rancho Santa Fe, California. Plaintiff O'Connor had his Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff O'Connor had three Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff O'Connor was required to create an account on MyPrepaidCenter.com and provide Defendant with his Private Information. In making his decision to create an account to gain full access to his Prepaid Cards, Plaintiff O'Connor reasonably expected that Defendant would safeguard his Private Information. Plaintiff O'Connor would not have created an account, nor would have provided Private Information, if he knew that the Private Information collected by Defendant would be at risk. Plaintiff Rogers has suffered damages and remains at a significant risk now that his Private Information has been leaked online.

Plaintiff Kelly Rogers

28. Plaintiff Kelly Rogers is a citizen of the State of Illinois and a is a resident of Wheaton, Illinois. Plaintiff Rogers had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Rogers had three Prepaid Cards serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Cards, Plaintiff Rogers was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Cards, Plaintiff Rogers reasonably expected that Defendant would safeguard her Private Information. Plaintiff Rogers would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Rogers has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Loushandra Vaughn

29. Plaintiff Loushandra Vaughn is a citizen of the State of Alabama and a is a resident of Mobile, Alabama. Plaintiff Vaughn had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Vaughn had at

least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Vaughn was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Vaughn reasonably expected that Defendant would safeguard her Private Information. Plaintiff Vaughn would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Vaughn has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Plaintiff Brittney Wood

30. Plaintiff Brittney Wood is a citizen of the State of Georgia and a is a resident of Lakemont, Georgia. Plaintiff Wood had her Private Information exfiltrated and compromised in the data breach announced by Defendant on or about October 31, 2022. Plaintiff Wood had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. To activate and use the Prepaid Card, Plaintiff Wood was required to create an account on MyPrepaidCenter.com and provide Defendant with her Private Information. In making her decision to create an account to gain full access to her Prepaid Card, Plaintiff Wood reasonably expected that Defendant would safeguard her Private Information. Plaintiff Wood would not have created an account, nor would have provided Private Information, if she knew that the Private Information collected by Defendant would be at risk. Plaintiff Wood has suffered damages and remains at a significant risk now that her Private Information has been leaked online.

Defendant Blackhawk

31. Defendant is a privately held corporation incorporated in the State of California. Defendant's headquarters is located at 6220 Stoneridge Mall Road, Pleasanton, California 94588. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

/ / /

/ / /

/ / /

III. JURISDICTION AND VENUE

32. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

33. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and this District through its headquarters, offices, parents, and affiliates.

34. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

35. Blackhawk is primarily engaged in providing "global branded payments" to its customers located within the United States and abroad, which includes gift cards, prepaid cards, other online payment options for employers and merchants, gaming, and gambling options.[7] Blackhawk is a privately held company with corporate headquarters in Pleasanton, California.

36. Blackhawk operates a consumer facing website located at www.blackhawknetwork.com ("Blackhawknetwork.com"). Customers or potential customers can then access MyPrepaidCenter.com through Blackhawknetwork.com.

37. To make use MyPrepaidCenter.com a customer must provide certain PII and PCD, specified in Blackhawk Network Privacy Notice ("Privacy Notice") that the policy pertains to all visitors, customers, users of apps, and users of prepaid cards and banded payments. Specifically, the Private Information, which Defendant collects, includes, but is not limited to:

- Contact information, such as name, email address, mailing address, fax, or phone number;
- Payment and financial information, such as credit or other payment card

[7] Blackhawk Network, https://blackhawknetwork.com/ (last visited on Nov. 15, 2022).

information, bank account, or billing address;

- Shipping address and related details;
- Resume, employment and education history, name and contact details, background details, and references when you apply to job postings or contact us about employment opportunities;
- Company and employment information;
- Subject to applicable local law restrictions, Social Security number or other national tax ID number (for clients and potential clients);
- Unique identifiers such as username, account number, or password;
- Preference information such as product wish lists, order history, or marketing preferences;
- Information about businesses, such as company name, size, or business type; and
- Demographic information, such as age, gender, interests and ZIP or postal code.[8]

38. Defendant also specifies in the Privacy Policy that it acts as the "Controller" of the Private Information supplied.

39. When they provided their Private Information to Defendant, Plaintiffs and Class Members relied on Defendant (a large, sophisticated internet branded payment program servicer) to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive PII and PCD at issue here, particularly where digital transactions are involved.

41. Defendant also recognized and voluntarily adopted additional duties to protect PII and PCD in its Privacy Policy which has been publicly posted to the internet.[9] In its Privacy Policy, Defendant also says the way it uses Private Information is at "the core of our obligations," that it

[8] Blackhawk Network, *Privacy Notice* (Apr. 4, 2022), https://blackhawknetwork.com/privacy-policy.
[9] *Id.*

will "not sell" information, and that it will use the information for "our own legitimate and lawful business interests."[10] Moreover, under its Frequently asked questions, in response to the question "is [MyPrepaidCenter.com] secured?" Defendant unequivocally answers "Yes. Information submitted through the Card website is protected by Secure Socket Layer (SSL) technology, which encrypts, or scrambles information submitted online."[11]

42. Despite these duties and promises, Defendant allowed data thieves to infect and infiltrate its MyPrepaidCenter.com website and steal the Private Information of thousands of its customers.

The Data Breach was foreseeable

43. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[12]

44. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

45. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

46. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep Private Information confidential and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from being compromised.

/ / /

[10] *Id.*

[11] Blackhawk Network, *Frequently Asked Questions*, https://www.myprepaidcenter.com/faq (last visited Nov. 15, 2022).

[12] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017.

The Data Breach

47. On or about October 31, 2022, Defendant notified various state Attorneys General, as well as Plaintiffs and Class Members, that, on September 12, 2022, Defendant discovered that MyPrepaidCenter.com experienced "irregular activity."[13]

48. The Notice informed Plaintiffs and Class Members that "[o]ur investigation revealed that irregular activity involved the unauthorized acquisition of information about you." This information included first and last name, email address, and phone numbers, but it also included information relating to the Pathward Prepaid Card(s), added on the MyPrepaidCenter.com profile such as card numbers, expiration dates, and CVV security codes.[14]

49. The Private Information exfiltrated in the Data Breach was unencrypted and captured directly from MyPrepaidCenter.com.[15]

50. Defendant claims it "blocked your impacted Pathward Prepaid Card(s)," yet it remained silent about what happened to the stolen Personal Information.[16]

51. Despite Defendant's promises that it: (i) would not disclose consumers' Private Information to unauthorized third parties; and (ii) would protect consumers' Private Information with adequate security measures, it appears that Defendant did not even implement, or require its third-party vendors to implement, basic security measures such as immediately encrypting PCD.

Blackhawk Experienced a Substantially Similar Data Breach Two Years Earlier

52. According to an earlier Security Incident Notification ("Notification"), on August 8, 2020, Blackhawk "detected some activity on its website GiftCards.com, indicating a possible 'brute force attack.'"[17]

53. Blackhawk conducted an investigation on August 14, 2020 and determined that the incident resulted in "unauthorized access" to a number of accounts.[18]

---

[13] Blackhawk Network, *Notice of Data Breach* (Oct. 31, 2022), https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Kate Lucente, *Security Incident Notification* (Aug. 28, 2020), https://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2020/itu-331656.pdf.

[18] *Id.*

54. The Notification also indicates similar Private Information was taken in the 2020 data breach as was taken in the Data Breach that is the subject of this class action:

> For any account accessed, the perpetrator(s) would have only had access to the customer's transaction history, original balance information for gift card(s), and account profile information, which includes customer name, email address, postal address, the name and contact information of any gift card recipient(s), and the last four digits of the credit card used in prior transactions. The perpetrator(s) would not have been able to access the full numbers of any gift cards purchased or the credit cards used to purchase gift cards through customer accounts. Further, the perpetrator(s) would not have been able to initiate a transaction using any stored cards without the Card Identification Number (CID) code for the particular credit card (which would not have been accessible through GiftCard.com).[19]

Securing PII and Preventing Breaches

55. Given Blackhawk's recent experience with data breaches, it should have been even more aware and taken further precautions to secure PII and other private information.

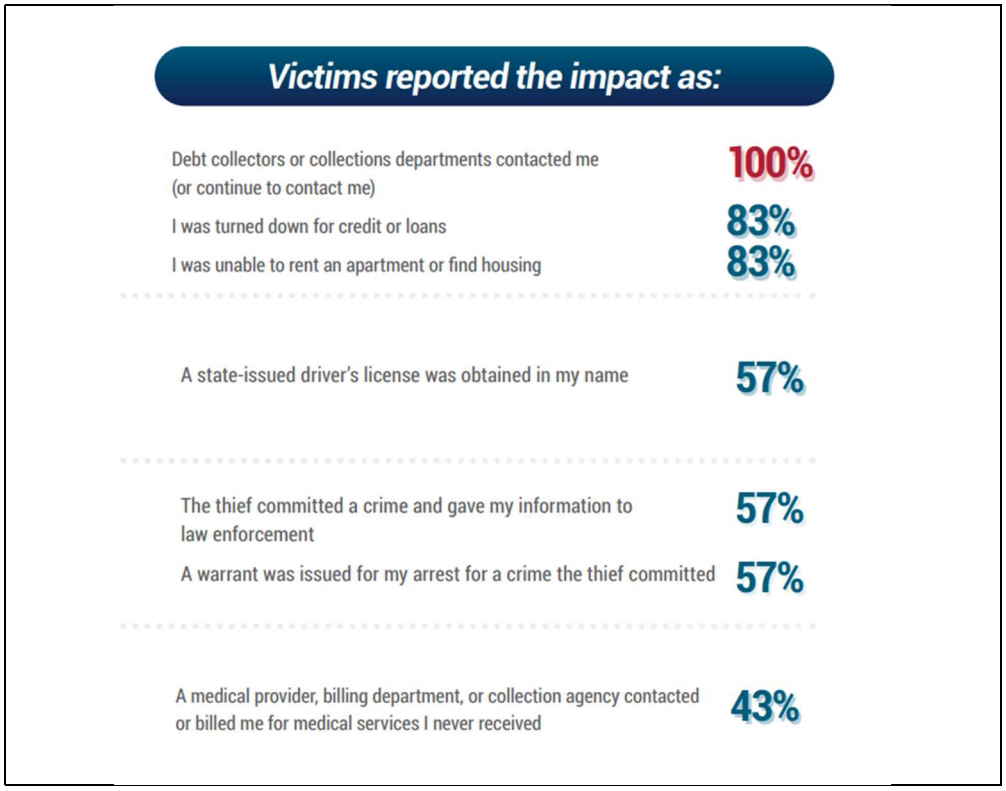
56. The financial fraud suffered by Plaintiffd and other customers demonstrates that Defendant, and/or its third party vendors, chose not to invest in the technology to encrypt payment card data (PCD) make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

57. These failures demonstrate a clear breach of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles PCD.

58. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[20]

[19] *Id.*

[20] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Nov. 15, 2022)



59. Plaintiffs and Class Members have experienced one or more of these harms as a result of the data breach.

60. Furthermore, theft of Private Information is also gravely serious. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

61. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

/ / /

[21] U.S. GOV'T ACCOUNTABILITY OFF., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, 12 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

62. Private Information and PCD are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

63. There is a strong probability that entire batches of stolen payment card information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

64. Plaintiffs and Class Members have and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

65. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

66. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

67. As a direct and proximate result of the Data Breach, Plaintiffs' PII and PCD was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiffs and Class Members.

68. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiffs and Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

69. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

70. Plaintiffs and Class Members also suffered a loss of value of their PII and PCD when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

71. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiffs and Defendant included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiffs and the Class Members did not get what they paid for.

72. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

73. Plaintiffs and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII and PCD;

b. Improper disclosure of their PII and PCD property;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of criminals;

d. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' Private Information for which there is a well-established and quantifiable national and international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

74. The substantial delay in providing notice of the Data Breach deprived Plaintiffs and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

Value of Personal Identifiable Information

75. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[22] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[23] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

76. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[24] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[25]

[22] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[23] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/

[24] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[25] *See* Data Coup, https://datacoup.com/ (last visited on Nov. 15, 2022).

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[26]

77. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

78. The fraudulent activity resulting from the Data Breach may not come to light for years and Plaintiffs and Class Members face a lifetime risk of fraud and identity theft as a result of the Data Breach.

79. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[27]

80. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, particularly given the sensitive nature of their purchases, and of the foreseeable consequences that would occur if Defendant's data security system was breached (as it had been as recently as 2020), including, specifically, the significant costs and risks that would be imposed on Plaintiff and Class Members as a result of a breach.

81. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur

[26] Nielsen, *Frequently Asked Questions, Nielsen Computer & Mobile Panel*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Nov. 15, 2022).

[27] U.S. Gov't Accountability Off., GAO 07737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

such damages in addition to any fraudulent use of their Private Information.

82. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to tens or hundreds of thousands of individual's detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

83. To date, Defendant has offered no credit monitoring or identity theft services. It has only offered to provide a replacement Pathway Prepaid Card(s). This is wholly inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

84. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures, and failure to adequately investigate, monitor, and audit its third-party vendors, to protect the Private Information of Plaintiff and Class Members.

Plaintiffs' Experience

85. Plaintiffs suffered actual injury from having their Private Information compromised and/or stolen as a result of the Data Breach.

86. Plaintiffs suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that they would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

87. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their personal and financial information – a form of intangible property that the Plaintiffs entrusted to Defendant for the purpose activating Prepaid Cards for use and which was compromised in, and as a result of, the Data Breach.

88. Plaintiffs suffered actual injury and damages when the stored value of their "useable" Pathward Prepaid Cards were reduced as a result of the Data Breach.

89. Plaintiffs suffer present and continuing injury arising from the substantially increased risk

of future fraud, identity theft and misuse posed by their personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

90. Plaintiffs have a continuing interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

91. As a result of the Data Breach, Plaintiffs made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiffs have spent several hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

92. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result of the release of their Private Information, which they believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiffs are very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. Plaintiffs suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiffs; (b) violation of their privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

94. As a result of the Data Breach, Plaintiffs anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

95. Plaintiffs bring this nationwide class action on behalf of themselves, and all others similarly

situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

96. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> "All persons Defendant identified as being among those individuals impacted by the Data Breach, including all persons who were sent a notice of the Data Breach."

97. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court

98. The Alabama Subclass which Plaintiffs seek to represent is defined as follows:

> "All persons residing in Alabama Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Alabama Subclass").

99. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

100. The California Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in California Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "California Subclass").

101. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

102. The Georgia Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in Georgia Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Georgia Subclass").

103. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

104. The Illinois Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in Illinois Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Illinois Subclass").

105. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

106. The Maine Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in Maine Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Maine Subclass").

107. Said definition may be further defined or amended by additional pleadings,

evidentiary hearings, a class certification hearing, and orders of this Court.

108. The Montana Subclass which Plaintiffs seek to represent comprises:

"All persons residing in Montana Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Montana Subclass").

109. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

110. The North Carolina Subclass which Plaintiffs seek to represent comprises:

"All persons residing in North Carolina Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "North Carolina Subclass").

111. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

112. The Ohio Subclass which Plaintiffs seek to represent comprises:

"All persons residing in Ohio Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Ohio Subclass").

113. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

114. The Pennsylvania Subclass which Plaintiffs seek to represent comprises:

"All persons residing in Pennsylvania Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Pennsylvania Subclass").

115. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

116. The Texas Subclass which Plaintiffs seek to represent comprises:

"All persons residing in Texas Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Texas Subclass").

117. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

118. The Virginia Subclass which Plaintiffs seek to represent comprises:

"All persons residing in Virginia Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Virginia Subclass").

119. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

120. The West Virginia Subclass which Plaintiffs seek to represent comprises:

> "All persons residing in West Virginia Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "West Virginia Subclass").

121. Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

122. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families, and Members of their staff.

123. Plaintiffs reserve the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

124. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of at least 165,727 current and former customers of Defendant whose sensitive data was compromised in Data Breach.[28]

125. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach

[28] Maine Attorney General, *Data Breach Notifications: Pathward, N.A.*, https://apps.web.maine.gov/online/aeviewer/ME/40/52a7dc3e-1734-4ea7-b1a8-6e8d49176588.shtml (last visited Nov. 15, 2022).

complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PCD;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

126. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

127. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class and have no interests antagonistic to those of

other Class Members. Plaintiffs' counsel are competent and experienced in litigating Class actions.

128. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

129. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

130. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW,

CAL. BUS. & PROF. CODE § 17200 et seq.

(On Behalf of the California Subclass and Nationwide Class)

131. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

132. For all Class members outside of the Alabama, California, Georgia, Illinois, Maine, Montana, North Carolina, Ohio, Pennsylvania, Texas, Virginia and West Virginia Subclasses,

these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. § 45.50.471, et seq.); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, et seq.); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, et seq.); Colorado— Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, et seq.); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, et seq.); Delaware—Consumer Fraud Act (Del. Code Ann. tit. 6, § 2511, et seq.); District of Columbia—D.C. Code § 28-3901, et seq.; Florida— Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, et seq.); Hawaii—Haw. Rev. Stat. § 480-1, et seq.); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, et seq.); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, et seq.); Iowa—Iowa Code § 7.14.16, et seq.); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, et seq.); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, et seq.); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, et seq.); Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, et seq.); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, et seq.); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, et seq.); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, et seq.); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, et seq., Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, et seq.); New Jersey—N.J. Stat. Ann. § 56:8-1, et seq.); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, et seq.); New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Dakota—N.D. Cent. Code § 51-15-01, et seq.); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, et seq.); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, et seq.); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, et seq.); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, et seq.); South Dakota—Deceptive Trade Practices and Consumer

Protection Law (S.D. Codified Laws § 37-24-1, et seq.); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47- 18-101, et seq.); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, et seq.); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, et seq.); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, et seq.); Wisconsin—Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, et seq.).

A. "Unfair" Prong

133. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." Camacho v. Auto Club of Southern California, 142 Cal. App. 4th 1394, 1403 (2006).

134. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individuals' data longer than necessary. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for customers' privacy and security.

135. Defendant did not need to collect the private data from its consumers to allow consumers' enhanced experiences of the products or services. It did so to track and target its customers and monetize the use of the data to enhance its profits. Defendant utterly misused this data and Private Information.

136. Defendant's conduct as alleged herein causes injuries to consumers, who do not receive a service consistent with their reasonable expectations.

137. Defendant's conduct as alleged herein causes injuries to consumers, entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

138. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal.

Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

139. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

140. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

141. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of Cal. Bus. & Prof. Code § 17200.

142. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

143. Defendant's conduct threatens consumers by exposing consumers' Private Information to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

144. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

145. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

146. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their decision to use Defendant's services in part based on Defendant's representations regarding their security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Inforrmation to Defendant reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased services. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the services, or would

not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Fraudulent" Prong

147. Cal. Bus. & Prof. Code § 17200, et seq. considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. Bank of the West v. Superior Court, 2 Cal. 4th 1254, 1267 (1992).

148. Defendant's advertising and representations that they adequately protect consumer's Private Information is likely to deceive members of the public into believing that Blackhawk can be entrusted with their Private Information, and that Private Information gathered by Blackhawk is not in danger of being compromised.

149. Defendant's representations about their services, as alleged in the preceding paragraphs, are false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

150. Defendant knew or should have known of its fraudulent conduct.

151. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of Cal. Bus. & Prof. Code § 17200 et seq.

152. Defendant could have implemented robust security measures to prevent the data breach but failed to do so.

153. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

154. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive advertising about the strength or adequacy of its security systems.

155. Likewise, Plaintiffs and the Class seek an order requiring Defendant to disclose such misrepresentations.

156. Plaintiffs and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiffs paid an unwarranted premium for services. Plaintiffs would not have used the services, if they had known that their use would put their Private Information at risk.

157. Injunction. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer's Private Information retained by Defendant. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

158. Cal. Bus. & Prof. Code § 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." Velazquez v. GMAC Mortg. Corp., 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

159. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates Cal. Bus. & Prof. Code § 1750 et seq.

160. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

161. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

162. Defendant knew or should have known of its unlawful conduct.

163. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of Cal. Bus. & Prof. Code §17200.

164. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

165. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct.

166. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

167. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for services. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the products and services, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

COUNT II

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT,

CAL. CIV. CODE § 1750, et seq.

(On Behalf of the California Subclass)

168. Plaintiff O'Connor repeats and re-alleges the allegations set forth in the preceding paragraphs and incorporates the same as if set forth herein at length.

169. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of services.

170. Defendant's unlawful conduct described herein was intended to increase sales to the consuming public and violated and continues to violate §§ 1770(a)(5), (a)(7), and (a)(9) of the

CLRA by representing that the products and services have characteristics and benefits which they do not have.

171. Defendant fraudulently deceived Plaintiff O'Connor and the California Subclass by representing that its services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff O'Connor and the California Subclass, specifically by advertising secure technology when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff O'Connor and the California Subclass and depriving them of their legal rights and money.

172. Defendant's claims about the products and services led and continues to lead consumers like Plaintiff O'Connor to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' Private Information.

173. Defendant knew or should have known that adequate security measures were not in place and that consumers' Private Information was vulnerable to a data breach.

174. Plaintiff O'Connor and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendant's false representations.

175. Plaintiff O'Connor and the California Subclass would not have purchased the products or used the services, or would have paid significantly less for the products and services, had they known that their Private Information was vulnerable to a data breach.

176. Defendant's actions as described herein were done with conscious disregard of Plaintiff O'Connor's rights, and Defendant was wanton and malicious in its concealment of the same.

177. Plaintiff O'Connor and the California Subclass have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff O'Connor paid for services advertised as secure, and consequentially entrusted Defendant with his Private Information, when Defendant in fact failed to institute adequate security measures

and neglected vulnerabilities that led to a data breach. Plaintiff O'Connor and the California Subclass would not have purchased the products and services, or would not have provided Defendant with their Private Information, had they known that their Private Information was vulnerable to a data breach.

178. Defendant should be compelled to implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiff O'Connor and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

179. At this time, Plaintiff O'Connor seeks injunctive relief under the CLRA pursuant to Cal. Civ. Code § 1782(d); but anticipates needing to amend the complaint and seek restitution.

COUNT III

(PENDING EXHAUSTION OF 30-DAY CURE PERIOD)

VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT ("CCPA"),

CAL. CIV. CODE § 1798.150 et seq.

(On Behalf of the California Subclass)

180. Plaintiff O'Connor repeats and re-alleges the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

181. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues in excess of $25,000,000.

182. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

183. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff O'Connor's and the California Subclass Members' nonencrypted Personal Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

184. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff O'Connor's and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so.

/ / /

185. As a direct and proximate result of Defendant's acts, Plaintiff O'Connor's and California Subclass Members' Personal Information, as defined in Cal. Civ. Code § 1798.81.5(d)(1)(A), including first and last name, email address, phone numbers, card numbers, expiration dates, and CVV security codes, was subjected to unauthorized access and exfiltration, theft, or disclosure.

186. Plaintiff O'Connor and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' Private Information, including Plaintiff O'Connor's and California Subclass Members' Private Information. Plaintiff O'Connor and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

187. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information under the CCPA.

188. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

189. Plaintiff O'Connor and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

190. On November 18, 2022, Plaintiff's counsel sent a notice letter to Defendant's registered address. Assuming Defendant cannot cure the Data Breach within 30 days, and Plaintiff believes such cure is not possible under these facts and circumstances, then Plaintiff intends to promptly amend this complaint to seek actual damages and statutory damages of $750 per customer record subject to the Data Breach on behalf of the California Subclass as permitted by the CCPA.

COUNT IV

DECEIT BY CONCEALMENT,

CAL. CIV. CODE §§ 1709 AND 1710

(On Behalf of the California Subclass)

191. Plaintiff O'Connor herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

192. Defendant knew or should have known that its security systems were inadequate to protect the Private Information of its consumers. Defendant experienced another data breach just a few years prior to the breach at issue, which alerted Defendant to the inadequacy of its internal data protections. Despite this knowledge, Defendant failed to adequately bolster its security systems, and allowed the second breach to occur, this time compromising consumer's Private Information. Further, the August 2020 data breach included names, email addresses, postal addresses, the names and contact information of any gift card recipient(s). The leak of this source code should have put Defendant on further notice that the data of its account holders was at imminent risk.

193. Specifically, Defendant had an obligation to disclose to its consumers that its security systems were not adequate to safeguard their Private Information. Defendant did not do so. Rather, Defendant deceived Plaintiff O'Connor and the California Subclass by concealing the vulnerabilities in its security system.

194. Even after Defendant discovered the data breach, it concealed it, and waited over an entire month before announcing it to the public so they could know and take precautions against the data breach.

195. Cal. Civ. Code § 1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore

constitutes deceit of Plaintiff O'Connor and the California Subclass.

196. Cal. Civ. Code § 1709 mandates that in willfully deceiving Plaintiff O'Connor and the California Subclass with intent to induce or alter their position to their injury or risk, Defendant is liable for any damage which Plaintiff O'Connor and the California Subclass thereby suffer.

197. As described above, Plaintiff O'Connor and the California Subclass have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Specifically, Plaintiff O'Connor and the Class have been subject to numerous attacks, increase in spam phone calls and emails. Defendant is liable for these damages.

COUNT V

VIOLATION OF ALABAMA'S DECEPTIVE TRADE PRACTICES ACT, ALA. CODE § 8-19-1 et seq.

(On Behalf of the Alabama Subclass)

198. Plaintiff Vaughn herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

199. Plaintiff Vaughn, Alabama Subclass members, and Defendant are "persons" as defined by Ala. Code § 8-9-1(10).

200. Defendant advertised, offered, or sold goods or services in Alabama and engaged in trade or commerce directly or indirectly affecting the people of Alabama, as defined by Ala. Code § 8-19-3(14).

201. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Ala. Code § 8-19-5, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another.

202. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Vaughn and Alabama Subclass members' Private Information,

which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vaughn's and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Vaughn's and Alabama Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vaughn's and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Vaughn's and Alabama Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Vaughn's and Alabama Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

203. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

204. Defendant intended to mislead Plaintiff Vaughn and Alabama Subclass members and induce them to rely on its own misrepresentations and omissions.

205. Defendant acted intentionally, knowingly, and maliciously to violate Alabama's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff Vaughn's and Alabama Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

206. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Vaughn and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

207. Plaintiff Vaughn and the Alabama Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $100 per Alabama Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT VI

VIOLATION OF GEORGIA'S FAIR BUSINESS PRACTICES ACT OF 1975, GA. CODE § 10-1-390 ET SEQ.

(On Behalf of the Georgia Subclass)

208. Plaintiff Brittney Wood herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

209. Plaintiff Wood, Georgia Subclass members, and Defendant are "persons" as defined by Ga. Code § 10-1-392(24).

210. Defendant advertised, offered, or sold goods or services in Georgia and engaged in trade or commerce directly or indirectly affecting the people of Georgia, as defined by Ga. Code

§ 10-1-392(28).

211. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Ga. Code § 10-1-393, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another.

212. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Wood's and Georgia Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Wood's and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Wood's and Georgia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Wood's and Georgia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Wood's and Georgia Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Wood's and Georgia Subclass members' Private information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

213. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

214. Defendant intended to mislead Plaintiff Wood and Georgia Subclass members and induce them to rely on its own misrepresentations and omissions.

215. Defendant acted intentionally, knowingly, and maliciously to violate Ga. Code § 10-1-390 et seq., and recklessly disregarded Plaintiff Wood's and Georgia Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

216. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Wood and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

217. Plaintiff Wood and the Georgia Subclass members seek all monetary and non-monetary relief allowed by law, including general and exemplary damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

/ / /

COUNT VII

VIOLATION OF ILLINOIS' CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT,

805 ILL. COMP. STAT. 505/1 et seq.

(On Behalf of the Illinois Subclass)

218. Plaintiffs Iglehart and Rogers herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

219. Plaintiffs Iglehart and Rogers, Illinois Subclass members, and Defendant are "persons" as defined by 805 Ill. Comp. Stat. 505/1(c).

220. Defendant advertised, offered, or sold goods or services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois, as defined by 805 Ill. Comp. Stat. 505/1(f).

221. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of 805 Ill. Comp. Stat. 505/2 and 805 Ill. Comp. Stat. 510/2, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

222. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to

protect Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Iglehart and Rogers' and Illinois Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

223. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and

ability to protect consumers' Private Information.

224. Defendant intended to mislead Plaintiffs Iglehart and Rogers and Illinois Subclass members and induce them to rely on its own misrepresentations and omissions.

225. Defendant also failed to implement and maintain reasonable security measures to protect Plaintiffs Iglehart and Rogers; and Illinois Subclass members's Private Information from unauthorized access, acquisition, destruction, use, modification, or disclosure, in violation of 805 Ill. Comp. Stat. 530/45.

226. Defendant acted intentionally, knowingly, and maliciously to violate 805 Ill. Comp. Stat. 505/2 and 805 Ill. Comp. Stat. 510/2, and recklessly disregarded Plaintiffs Iglehart and Rogers' and Illinois Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

227. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Iglehart and Rogers' and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

228. Plaintiffs Iglehart and Rogers' and the Illinois Subclass members seek all monetary and non- monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT VIII

VIOLATION OF MAINE'S UNFAIR TRADE PRACTICES ACT,

ME. STAT. TIT. 5, § 205-A ET SEQ.

(On Behalf of the Maine Subclass)

229. Plaintiff Edwards herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

230. Plaintiff Edwards, Maine Subclass members, and Defendant are "persons" as defined by Me. Stat. tit. 5, § 206(2).

231. Defendant advertised, offered, or sold goods or services in Maine and engaged in trade or commerce directly or indirectly affecting the people of Maine, as defined by Me. Stat. tit. 5, § 206(3).

232. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Me. Stat. tit. 5, § 207, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

233. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Edward's and Maine Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Edward's and Maine Subclass members' Private

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Edwards's and Maine Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Edward's and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Edward's and Maine Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Edwards's and Maine Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

234. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

235. Defendant intended to mislead Plaintiff Edwards and Maine Subclass members and induce them to rely on its own misrepresentations and omissions.

236. Defendant acted intentionally, knowingly, and maliciously to violate Me. Stat. tit. 5 § 205-A et seq., and recklessly disregarded Plaintiff Edwards's and Maine Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

/ / /

237. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Edwards and Maine Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

238. Plaintiff Edwards and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT IX

VIOLATION OF MONTANA'S UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT OF 1973,

MONT. CODE ANN. § 30-14-101 et seq.

(On Behalf of the Montana Subclass)

239. Plaintiffs Grose and Hulsey herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

240. Plaintiffs Grose and Hulsey, Montana Subclass members, and Defendant are "persons" as defined by Mont. Code. Ann. § 30-14-102(6).

241. Defendant advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by Mont. Code. Ann. § 30-14-102(8).

242. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mont. Code. Ann. § 30-14-103, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

/ / /

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

243. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Grose and Hulsey's and Montana Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Grose and Hulsey's and Montana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Grose and Hulsey's and Montana Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Grose and Hulsey's and Montana

Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Grose and Hulsey's and Montana Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Grose and Hulsey's and Montana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

244. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

245. Defendant intended to mislead Plaintiffs Grose and Hulsey and Montana Subclass members and induce them to rely on its own misrepresentations and omissions.

246. Defendant acted intentionally, knowingly, and maliciously to violate Mont. Code. Ann. § 30-14-101 et seq., and recklessly disregarded Plaintiffs Grose and Hulsey's and Montana Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

247. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Grose and Hulsey and Montana Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's products and services; loss of the value of access to their PII; and the value of identity protection services made necessary by the data breach.

248. Plaintiffs Grose and Hulsey and the Montana Subclass members seek all monetary and non- monetary relief allowed by law, including the greater of actual damages or $500 per

Montana Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT X

N.C. GEN. STAT. § 75-1.1 et seq.

(On Behalf of the North Carolina Subclass)

249. Plaintiff Mieir herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

250. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. § 75-1.1(b).

251. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of N.C. Gen. Stat. § 75-1.1, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

252. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Mieir's and North Carolina Subclass members' Private Information, which was a direct and proximate cause of the data breach;

/ / /

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Mieir's and Montana Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumer Private Information.

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Mieir's and North Carolina Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Mieir's and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Mieir's and North Carolina Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Mieir's and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

253. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

/ / /

254. Defendant intended to mislead Plaintiff Mieir and North Carolina Subclass members and induce them to rely on its own misrepresentations and omissions.

255. Defendant acted intentionally, knowingly, and maliciously to violate N.C. Gen. Stat. § 75-1.1, and recklessly disregarded Plaintiff Mieir's and North Carolina Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

256. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Mieir and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the data breach.

257. Plaintiff Mieir and the North Carolina Subclass members seek all monetary and non- monetary relief allowed by law, including the treble damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT X

VIOLATION OF OHIO'S CONSUMER SALES PRACTICES ACT,

OHIO REV. CODE ANN. § 1345.01 ET SEQ.

(On Behalf of The Ohio Subclass)

258. Plaintiffs Ferryman and Hundley herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

259. Plaintiffs Ferryman and Hundley, Ohio Subclass members, and Defendant are "persons" as defined by Ohio Rev. Code Ann. § 1345.01(B).

260. Defendant advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

/ / /

261. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Ohio Rev. Code Ann. § 1345.02, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

262. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

/ / /

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Ferryman and Hundley's and Ohio Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

263. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

264. Defendant intended to mislead Plaintiffs Ferryman and Hundley and Ohio Subclass members and induce them to rely on its own misrepresentations and omissions.

265. Defendant acted intentionally, knowingly, and maliciously to violate Ohio Rev. Code Ann. § 1345.01 et seq, and recklessly disregarded Plaintiffs Ferryman and Hundley's and Ohio Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

266. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Ferryman and Hundley and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased,

imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

267. Plaintiffs Ferryman and Hundley and the Ohio Subclass members seek all monetary and non- monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT XI

VIOLATION OF PENNSYLVANIA'S UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, 73 PA. CONS. STAT. § 201-1 ET SEQ.

(On Behalf of the Pennsylvania Subclass)

268. Plaintiffs Drevenak and Mikec herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

269. Plaintiffs Drevenak and Mikec, Pennsylvania Subclass members, and Defendant are "persons" as defined by 73 Pa. Cons. Stat. § 201-2(2).

270. Defendant advertised, offered, or sold goods or services in Pennsylvania and engaged in trade or commerce directly or indirectly affecting the people of Pennsylvania, as defined by 73 Pa. Cons. Stat. § 201-2(3).

271. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of 73 Pa. Cons. Stat. § 201-3, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other

than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

272. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information; and

/ / /

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

273. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

274. Defendant intended to mislead Plaintiffs Drevenak and Mike and Pennsylvania Subclass members and induce them to rely on its own misrepresentations and omissions.

275. Defendant acted intentionally, knowingly, and maliciously to violate 73 Pa. Cons. Stat. § 201-1 et seq., and recklessly disregarded Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

276. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Drevenak and Mikec's and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the data breach.

277. Plaintiffs Drevenak and Mikec and the Pennsylvania Subclass members seek all monetary and non- monetary relief allowed by law, including the greater of actual damages or $100 per Pennsylvania Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

/ / /

/ / /

/ / /

COUNT XII

VIOLATION OF TEXAS'S DECEPTIVE TRADE PRACTICES – CONSUMER PROTECTION ACT, TEX. BUS. & COM. CODE ANN. §17.41 ET SEQ.

(On Behalf of the Texas Subclass)

278. Plaintiff Cortez herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

279. Plaintiff Cortez, Texas Subclass members, and Defendant are "persons" as defined by Tex. Bus. & Com. Code Ann. § 17.45(2).

280. Defendant advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code Ann. § 17.45(6).

281. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Tex. Bus. & Com. Code Ann. § 17.46, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

282. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Cortez's and Texas Subclass members' Private Information, which

was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Cortez's and Texas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Cortez's and Texas Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

283. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

284. Defendant intended to mislead Plaintiff Cortez and Texas Subclass members and induce them to rely on its own misrepresentations and omissions.

285. Defendant acted intentionally, knowingly, and maliciously to violate Tex. Bus. & Com. Code Ann. § 17.41 et seq., and recklessly disregarded Plaintiff Cortez's and Texas Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

286. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Cortez and Texas Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

287. Plaintiff Cortez and the Texas Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT XIII

VIOLATION OF VIRGINIA'S CONSUMER PROTECTION ACT OF 1997, VA. CODE. ANN. § 59.1-196 ET SEQ.

(On Behalf of the Virginia Subclass)

288. Plaintiff Jenkins herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

289. Plaintiff Jenkins, Virginia Subclass members, and Defendant are "persons" as defined by Va. Code. Ann. § 59.1-198.

290. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Va. Code. Ann.. § 59.1-200, including:

/ / /

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

291. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Jenkins' and Virginia Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jenkins' and Virgnia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Jenkins' and Virginia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jenkins' and Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Jenkin's and Virginia Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Jenkins' and Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

292. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

293. Defendant intended to mislead Plaintiff Jenkins and Virginia Subclass members and induce them to rely on its own misrepresentations and omissions.

294. Defendant acted intentionally, knowingly, and maliciously to violate Va. Code. Ann. § 59.1-200, and recklessly disregarded Plaintiff Jenkins' and Virginia Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

295. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Jenkins and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the data breach.

296. Plaintiff Jenkins and the Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 per Virginia Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT XIV

VIOLATION OF WEST VIRGINIA'S CONSUMER CREDIT AND PROTECTION ACT, W. VA. CODE § 46A-6-101 ET SEQ.

(On Behalf of the West Virginia Subclass)

297. Plaintiffs Linger and Linger herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

298. Plaintiffs Linger and Linger, West Virginia Subclass members, and Defendant are "persons" as defined by W. Va. Code § 46a-6-101 et seq.

299. Defendant advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46-6-102(6).

300. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of W. Va. Code § 46A-6-104, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

/ / /

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

301. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Linger and Linger's and West Virginia Subclass members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Linger and Linger and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Linger and Linger's and West Virginia Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Linger and Linger and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Linger and Linger's and West Virginia Subclass members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff Linger and Linger's and West Virginia Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

302. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

303. Defendant intended to mislead Plaintiffs Linger and Linger and West Virginia Subclass members and induce them to rely on its own misrepresentations and omissions.

304. Defendant acted intentionally, knowingly, and maliciously to violate W. Va. Code § 46A-6-101 et seq., and recklessly disregarded Plaintiff Linger and Linger's and West Virginia Subclass members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

305. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Linger and Linger and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the data breach.

306. Plaintiff Linger and Linger and the West Virginia Subclass members seek all monetary and non- monetary relief allowed by law, including the greater of actual damages or $200 per West Virginia Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT XV

Negligence

(On behalf of Plaintiffs and Class Members)

307. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

308. Defendant solicited and gathered the Private Information, including the PCD, of Plaintiffs and Class Members to facilitate sales transactions.

309. Defendant knew, or should have known, of the risks inherent in collecting the PII and PCD of Plaintiffs and the Class Members and the importance of adequate security. Defendant also knew about numerous, well-publicized payment card data breaches involving other national retailers, including its own similar data breach from two years ago.

310. Defendant owed duties of care to Plaintiffs and the Class Members whose Private Information was entrusted to it. Defendant's duties included the following:

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

b. To exercise reasonable care in selecting its third-party vendors and monitoring and auditing their data security practices ensuring compliance with legal and industry standards and obligations;

c. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the PCI DSS and consistent with industry-standard practices;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiffs and Class Members of the data breach.

311. By collecting this data and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in case of a data breach.

312. Defendant's duty of care extended to ensuring that any third-party vendors it hired and that had exposure to the Private Information of Plaintiff and Class Members would implement adequate measures to prevent and detect cyber intrusions.

313. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class Members, it had a duty to adequately protect their Private Information.

314. Defendant owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

315. Defendant had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

316. Defendant knew, or should have known, that its computer systems and security practices did not adequately safeguard the Private Information of Plaintiff and the Class Members.

317. Defendant knew, or should have known, that the computer systems and security practices of its third-party vendors did not adequately safeguard the Private Information of Plaintiff and the Class Members.

318. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and the Class Members.

319. Defendant breached its duties of care by failing to provide prompt notice of the data breach to the persons whose PII and PCD were compromised.

320. Defendant acted with reckless disregard for the security of the Private Information of Plaintiffs and the Class Members because Defendant knew or should have known that its computer systems and data security practices, and those of its third-party vendors, were not adequate to safeguard the PII and PCD that that it collected, which hackers targeted in the Data Breach.

321. Defendant acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

/ / /

322. Defendant had a special relationship with Plaintiffs and the Class Members. Plaintiff's and the Class Members' willingness to entrust Defendant with their Private Information was predicated on the mutual understanding that Defendant would implement adequate security precautions. Moreover, Defendant was in an exclusive position to protect its systems (and the Private Information) from attack. Plaintiffs and Class Members relied on Defendant to protect their Private Information.

323. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PII and PCD. Defendant's misconduct included failing to:

a. Secure its e-commerce website;

b. Secure access to its and its vendors' servers;

c. Audit and monitor its vendors;

d. Comply with industry standard security practices;

e. Follow the PCI-DSS standards;

f. Encrypt PCD at the point-of-sale and during transit;

g. Employ adequate network segmentation;

h. Implement adequate system and event monitoring;

i. Utilize modern payment systems that provided more security against intrusion;

j. Install updates and patches in a timely manner; and

k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

324. Defendant also had independent duties under the FTC Act and state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' PII and PCD and promptly notify them about the data breach.

325. Defendant breached the duties it owed to Plaintiffs and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

/ / /

b. By failing to implement adequate security systems, protocols, and practices sufficient to protect their PII and PCD both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the Data Breach, and

d. By failing to timely and accurately disclose that the PII and PCD of Plaintiffs and the Class had been improperly acquired or accessed.

326. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

327. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

328. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was reasonably foreseeable.

329. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

330. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT XVI

Intentional Misrepresentation

(On Behalf of Plaintiffs and Class Members)

331. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

332. Defendant has represented, through its privacy policy, that Defendant "safeguards" all information provided by consumers, particularly "personal information."[29]

/ / /

/ / /

[29] Blackhawk Network, *Privacy Policy* (Apr. 4, 2022) https://blackhawknetwork.com/privacy-policy.

333. Defendant claims that they are "strongly committed to protecting the privacy of those who entrust [them] with their personal information."[30]

334. Defendant in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

335. Defendant's misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' PII. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making his or her decision to use Defendant's services.

336. At all relevant times when such misrepresentations were made, Defendant knew or should have known that the representations were misleading.

337. Defendant intended for Plaintiffs and the Class to rely on the representations of its security systems, as evidenced by Defendant's intentional marketing of safe and secure services.

338. Plaintiffs and members of the Class reasonably and justifiably relied on Defendant's intentional misrepresentations when using its services, and had they known the truth, they would not have used the services or would not have given Defendant their PII.

339. Defendant was negligent in its representations that it would provide the highest level of security for consumers.

340. As a direct and proximate result of Defendant's intentional misrepresentations, Plaintiffs and members of the Class have suffered injury in fact.

COUNT XVII

Breach of Implied Contract

(On behalf of Plaintiffs and Class Members)

341. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

/ / /

[30] Blackhawk Network Policies and Approaches, quoting, "Privacy and Security" available at: https://blackhawknetwork.com/responsible-practices (last accessed on Nov. 8, 2022).

342. When Plaintiffs and Class Members provided their PII and PCD to Defendant in making purchases on its website, they entered into implied contracts under which Defendant agreed to protect their PII and PCD and timely notify them in the event of a data breach.

343. Defendant invited its customers, including Plaintiffs and the Class, to make purchases of Prepaid Gift cards on its website using payment cards in order to increase sales by making purchases more convenient.

344. An implicit part of the offer was that Defendant would safeguard their Private Information using reasonable or industry-standard means and would timely notify Plaintiffs and the Class in the event of a data breach.

345. Defendant also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiffs and the Class in several ways, as described above.

346. Based on the implicit understanding and also on Defendant's representations, Plaintiffs and the Class accepted the offers and provided Defendant with their PII and PCD by using their payment cards in connection with purchases on the Defendant website during the period of the data breach.

347. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs' and Class Members' PII and PCD through, among other things, its Privacy Notice.

348. Defendant further demonstrated an intent to safeguard the Private Information of Plaintiffs and Class Members through its conduct. No reasonable person would provide sensitive, non-public information without the implicit understanding that the organization would maintain that information as confidential.

349. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

350. Plaintiffs and Class Members would not have provided their PII and PCD to Defendant had they known that Defendant would not safeguard their PII and PCD as promised or provide timely notice of a data breach.

351. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

352. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the Data Breach.

353. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breaches of its implied contracts with them.

COUNT XVII

Unjust Enrichment

(on behalf of Plaintiff and Class Members)

354. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

355. This claim is brought in the alternative to Plaintiffs' claim for breach of implied contract.

356. Defendant funds its data security measures entirely from its general revenue, including payments made by Plaintiffs and Class Members.

/ / /

357. As such, a portion of the payments made by Plaintiffs and Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

358. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods (Prepaid Gift Cards, specifically) and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

359. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information

of Plaintiff and Class Members for business purposes.

360. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information and instead directing those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

361. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

362. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

363. Plaintiffs and the Class have no adequate remedy at law.

364. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members of the Class conferred on it.

365. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and the Class overpaid, plus attorneys' fees, costs, and interest thereon.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing one of the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Classes requested

herein;

c. Judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, attorney's fees, statutory costs, and such other and further relief as is just and proper;

d. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

e. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

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

Respectfully Submitted,

DATED: November 28, 2022

By /s/ Kiley L. Grombacher

BRADLEY/GROMBACHER LLP
Marcus J. Bradley, Esq.
Kiley L. Grombacher, Esq.
Lirit A. King, Esq.
Attorneys for Plaintiffs and the Proposed Class