

Patrick. R. Leverty, Esq.
NV Bar No. 8840
pat@levertylaw.com
William R. Ginn, Esq.
NV Bar No. 6989
bill@levertylaw.com
LEVITY & ASSOCIATES LAW, CHTD.
832 Willow Street
Reno, NV 89502
Telephone: (775)322-6636

William B. Federman
(admitted *pro hac vice*)
Kennedy M. Brian
(admitted *pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

Attorneys for Plaintiffs and the Class

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEVADA**

**KEVIN MEAGHER and REBECCA
DAWSON** on behalf of themselves and on
behalf of all other similarly situated individuals,

Plaintiffs,

v.

**KTC HOLDING COMPANY F/K/A THE
KINGDOM TRUST COMPANY,**

Defendant.

Case No. 2:24-cv-01630-CDC-MDC

**FIRST AMENDED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

Plaintiff Kevin Meagher and Plaintiff Rebecca Dawson (collectively, “Plaintiffs”),
individually and on behalf of all other similarly situated individuals (the “Class” or “Class
Members,” as defined below), by and through their undersigned counsel, file this First Amended

1 Class Action Complaint against KTC Holding Company f/k/a The Kingdom Trust Company
2 (“Kingdom Trust” or “Defendant”) and allege the following based on personal knowledge of
3 facts, upon information and belief, and based on the investigation of their counsel as to all other
4 matters.

5 **I. NATURE OF THE ACTION**

6 1. Plaintiffs bring this class action lawsuit against Kingdom Trust for its negligent
7 failure to protect and safeguard Plaintiffs’ and the Class’s (**approximately 31,862 individuals**)
8 highly sensitive personally identifiable information (“PII”). As a result of Kingdom Trust’s
9 negligence and insufficient data security, cybercriminals easily infiltrated Defendant’s
10 inadequately protected network and stole the PII of Plaintiffs and the Class (the “Data Breach” or
11 “Breach”). Now, Plaintiffs’ and the Class’s PII is in the hands of cybercriminals who will
12 undoubtedly use their PII for nefarious purposes for the rest of their lives.

13 2. According to Kingdom Trust, on or around March 1, 2024, Kingdom Trust become
14 aware of potential unauthorized access to its network.¹

15 3. After an investigation, Defendant definitively determined “certain data was subject
16 to unauthorized access.”²

17 4. According to Kingdom Trust, the Data Breach was the result of an unauthorized
18 SIM swap, through which an unauthorized threat actor gained access to certain data on Kingdom
19 Trust’s systems and networks.³

20 5. “SIM swapping is a legitimate practice where someone can transfer access to
21 smartphone information from the owner's device to theirs. While SIM swapping can occur
22 between consenting parties, it is also used by criminals to gain access to an unsuspecting person's
23 phone...SIM swap fraud exploits this by deceiving carriers into transferring a mobile number
24 from its owner's device to another device with a different SIM card. Transferring the number
25 sends calls, voicemails, and texts to the new device rather than the owner's device. This allows
26

27 ¹ Exs. 1–2 (Plaintiffs’ Notice of Data Breach Letters).

28 ² *Id.*

³ <https://mm.nh.gov/files/uploads/doj/remote-docs/kingdom-trust-20240827.pdf>.

1 the identity thief to intercept messages used for security checks, such as one-time password
2 (OTP) messages. Using this method, identity thieves can impersonate victims to gain access to
3 sensitive personal, business, and financial data, such as bank accounts and social media
4 accounts.”⁴

5 6. “After a SIM swap, the threat actor often enters the account and downloads sizable
6 quantities of data in a short period of time from cloud storage or other data-driven applications,
7 such as Microsoft SharePoint and OneDrive. By the time the organization has removed the threat
8 actor’s access, the threat actor already possesses the organization’s information.”⁵

9 7. “Executives are attractive targets for cybercriminals. Their privileged access to a
10 corporate network is inviting to cybercriminals looking to exploit valuable data, corporate
11 networks or any means to extort large sums of money.”⁶

12 8. Kingdom Trust confirmed PII may have been copied from its network because of
13 the Breach.⁷ However, if not to steal personal information, why else would cybercriminals go
14 through the trouble of perpetrating a data breach?

15 9. The PII stolen in the Data Breach included highly sensitive information such as:
16 names, dates of birth, email addresses, phone numbers, and Social Security numbers, among other
17 sensitive data (collectively, “Private Information”).⁸

18 10. Defendant began sending Notice of Data Breach Letters to victims of the Data
19 Breach in or around August 2024.⁹

20 11. Due to Defendant’s negligence, cybercriminals stole and obtained everything they
21 needed to commit identity theft and fraud and wreak havoc on the financial and personal lives of
22 thousands of individuals.

23
24
25 ⁴ <https://www.twilio.com/en-us/blog/sim-swap-fraud>.

26 ⁵ https://www.aon.com/cyber-solutions/aon_cyber_labs/a-simple-attack-a-look-into-recent-sim-swap-attack-trends/.

27 ⁶ <https://woodrufflawyer.com/insights/cyber-sim-swapping>.

28 ⁷ *Id.*

⁸ Exs. 1–2.

⁹ *Id.*

12. Now, and for the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

13. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

14. In sum, Plaintiffs and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because (i) Kingdom Trust failed to protect Plaintiffs' and the Class's Private Information, allowing a massive and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach, accessed Private Information that they will disseminate on the dark web (if they have not done so already); and (iii) Kingdom Trust offered credit monitoring to Class Members, an offer it need not make if no Private Information was stolen and at an imminent risk of misuse.

15. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

16. Plaintiff **Kevin Meagher** is an individual domiciled in Raleigh, North Carolina. Plaintiff Meagher received a Notice of Data Breach Letter from Kingdom Trust dated August 21, 2024, notifying him that his Social Security number and name were "subject to unauthorized access."¹⁰

17. Plaintiff **Rebecca Dawson** is an individual domiciled in Los Angeles, California.

¹⁰ Ex. 1.

1 Plaintiff Dawson received a Notice of Data Breach Letter from Kingdom Trust dated August 21,
2 2024, notifying her that her full name, date of birth, email, and mobile number were “subject to
3 unauthorized access.”¹¹

4 18. Defendant **Kingdom Trust** is a corporation domesticated in the State of Nevada
5 with its principal place of business located at 7336 W. Post Road, Suite #111, Las Vegas, NV
6 89118. Defendant maintains and transacts substantial business across the state of Nevada and the
7 United States.

8 **III. JURISDICTION AND VENUE**

9 19. This Court has subject matter jurisdiction pursuant to the Class Action Fairness
10 Act of 2005 (“CAFA”), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of
11 \$5,000,000 exclusive of interest and costs, there are more than one hundred putative Class
12 Members, and minimal diversity exists because many putative Class Members are citizens of a
13 different state than Defendant. Indeed, Notice of Data Breach Letters were sent to Data Breach
14 victims located in Iowa, North Carolina, Massachusetts, Washington D.C., Maryland, California,
15 Oregon, New Mexico, Rhode Island, New York, and New Hampshire.¹²

16 20. This Court has personal jurisdiction over Defendant because Defendant is a
17 corporation domesticated in Nevada; has its principal place of business in this District; conducts
18 substantial business in this District through its headquarters, offices, and affiliates; engaged in the
19 conduct at issue here in this District; and/or otherwise has substantial contacts with this District
20 and purposely availed itself to the Courts in this District.

21 21. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and
22 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities
23 within this District.

24
25
26
27

¹¹ Ex. 2.

28 ¹² Exs. 1–2; <https://mm.nh.gov/files/uploads/doj/remote-docs/kingdom-trust-20240827.pdf>.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business.

22. Kingdom Trust serves as an independent qualified custodian for the assets of clients of registered investment advisors, broker-dealers and investment sponsors, as well as their Individual Retirement Accounts (IRAs), non-qualified plans and qualified defined contribution 401(k) plans.¹³

23. Kingdom Trust claims to provide “industry-leading technology to allow clients to have complete control over their Self-Directed IRA and other retirement and non-retirement accounts.”¹⁴

24. Kingdom Trust is estimated to employ over 100 individuals and have annual revenue in excess of \$25 million. In other words, Kingdom Trust could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

25. When conducting an internet search for “Kingdom Trust Company,” no website associated with Kingdom Trust Company appears. Rather, all searches for Kingdom Trust are directed to www.choiceapp.io (“Choice”), custodied by Digital Trust.¹⁵ According to Choice’s website, Digital Trust was formerly the Kingdom Trust Company.¹⁶ Despite this indication on Choice’s website, Kingdom Trust claims the proper Defendant to Plaintiffs’ lawsuit is KTC Holding Company, necessitating Plaintiffs’ Amended Complaint.

26. Kingdom Trust is most likely obfuscating its true identity because the Financial Crimes Enforcement Network (“FinCEN”) recently assessed a \$1.5 million civil money penalty against Kingdom Trust for willful violations of the Bank Secrecy Act in 2023.¹⁷

27. In connection with this penalty, Kingdom Trust admitted it “willfully failed to accurately and timely report hundreds of transactions to FinCEN involving suspicious activity by

¹³ See <https://www.choiceapp.io/about-digital-trust>.

¹⁴ *Id.*

¹⁵ <https://www.choiceapp.io/about-digital-trust>.

¹⁶ See <https://tktc.accessasc.com/Account/Login> (“Digital Trust (Formerly The Kingdom Trust Company”).

¹⁷ <https://www.fincen.gov/news/news-releases/fincen-assesses-15-million-civil-money-penalty-against-kingdom-trust-company>.

its customers, including transactions with connections to a trade-based money laundering scheme and multiple securities fraud schemes that were the subject of both criminal and civil actions. These failures stemmed from Kingdom Trust's severely underdeveloped process for identifying and reporting suspicious activity."¹⁸

B. Defendant's Collection of Plaintiffs' and the Class's Private Information.

28. Kingdom Trust provides financial services to businesses, including The Loan Source, Inc. and ACAP SME, LLC, which provided services to Plaintiffs and Class Members related to the U.S. Small Business Administration's Paycheck Protection Program.¹⁹ Through these relationships, Kingdom Trust accessed and acquired the Private Information of Plaintiffs and the Class.²⁰

29. In the ordinary course of business, Kingdom Trust receives the Private Information of individuals, such as Plaintiffs and the Class, from the entities and individuals that utilize Kingdom Trust's services.

30. Kingdom Trust obtains, collects, uses, and derives a benefit from the Private Information of Plaintiffs and Class Members.

31. Kingdom Trust uses the Private Information it collects to provide services, making a profit therefrom.

32. Kingdom Trust would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's Private Information.

33. By collecting Plaintiffs' and the Class's Private Information, Kingdom Trust assumed legal and equitable duties to Plaintiffs and the Class to protect and safeguard their Private Information from unauthorized access and intrusion.

34. Kingdom Trust recognizes this duty and makes the following claim on Choice's website regarding its protection of sensitive data:

¹⁸ *Id.*

¹⁹ Exs. 1–2.

²⁰ *Id.*

SECURITY

Digital Trust maintains a comprehensive disaster and security plan and a thorough set of controls and safeguards to ensure the security of our systems, website, data and real estate. The plan includes policies for operating the business as well as critical systems that need to be in place to conduct business. The plan is reviewed and tested annually to ensure all components are working properly and the systems will be functional in a timely manner if the need arises.²¹

35. Indeed, Kingdom Trust states in the Notice of Data Breach Letters sent to Plaintiffs and the Class, “[t]he privacy and security of the personal information we maintain is of the utmost importance to Kingdom Trust.”²²

36. Kingdom Trust’s assurances of maintaining high standards of cybersecurity make it evident that Kingdom Trust recognized it had a duty to use reasonable measures to protect the PII that it collected and maintained.

37. Kingdom Trust violated its own privacy statement and assurances by failing to adopt reasonable and appropriate data security practices and procedures including administrative procedures, physical security, and technical controls to safeguard Plaintiffs’ and the Class’s Private Information.

38. As a result, Plaintiffs’ and Class Members’ Private Information was accessed and stolen from Kingdom Trust’s inadequately secured data systems in a massive and preventable Data Breach.

C. Kingdom Trust’s Massive and Preventable Data Breach.

39. On or around March 1, 2024, Kingdom Trust became aware of potential unauthorized access to its network.²³

40. After detecting the Breach, Kingdom Trust claims it retained external cybersecurity professionals and notified law enforcement.²⁴

41. In a letter to the New Hampshire Attorney General, Kingdom Trust stated the

²¹ <https://www.choiceapp.io/about-digital-trust>.

²² Exs. 1–2.

²³ *Id.*

²⁴ *Id.*

1 following:²⁵

2
3 On or about March 1, 2024, Kingdom Trust became aware of potential unauthorized access on its network.
4 After identifying the incident, Kingdom Trust engaged our firm and third-party independent cybersecurity
5 experts to conduct a thorough investigation of the nature and scope of the incident and to assist in the
6 remediation efforts. Kingdom Trust also notified law enforcement.

7 Kingdom Trust's investigation revealed that, as a result of an unauthorized SIM swap, a threat actor gained
8 access to certain data that may have been copied from its network. Kingdom Trust conducted an extensive
9 forensic investigation and manual document review and discovered that certain personal information was
10 included within the impacted data. Further, Kingdom Trust notified its clients and worked with them to
11 identify the list of potentially impacted individuals and the most recent contact information to notify these
12 individuals. This process was completed on or about August 1, 2024.

13 42. "SIM swaps work by a hacker convincing a cell phone carrier to switch a mobile
14 number to a SIM in the hacker's possession. After gaining control of the phone number, the hacker
15 can change the passwords to all the accounts that use that number for two-factor or multifactor
16 verification."²⁶

17 43. Despite discovering the Data Breach on March 1, 2024, Kingdom Trust did not
18 begin notifying victims of the Data Breach until on or around August 1, 2024.²⁷

19 44. It was negligent for Kingdom Trust not to notify victims of the Data Breach prior
20 to August 1, 2024. Reason being, it is evident Kingdom Trust had the ability to notify victims of
21 the Data Breach as soon as July 12, 2024, because that is when Kingdom Trust began notifying
22 State Attorney Generals of the number of Data Breach victims residing in each state.²⁸

23 45. Regardless, Kingdom Trust unequivocally admitted in the Notice of Data Breach
24 Letters sent to Plaintiffs and the Class that "certain data was subject to unauthorized access" and
25 that sensitive data "may have been copied from [its] network."²⁹

26 46. The Private Information accessed and stolen in the Data Breach included at least:

27 ²⁵ <https://mm.nh.gov/files/uploads/doj/remote-docs/kingdom-trust-20240827.pdf>.

28 ²⁶ <https://www.avast.com/c-sim-swap-scam>.

²⁷ *Id.*

²⁸ <https://mm.nh.gov/files/uploads/doj/remote-docs/kingdom-trust-20240827.pdf>;
<https://www.mass.gov/doc/2024-1305-kingdom-trust/download>.

²⁹ Exs. 1–2.

names, dates of birth, email addresses, phone numbers, and Social Security numbers.³⁰

47. In recognition of the severity of the Data Breach, and the imminent risk of harm Plaintiffs and the Class face, Kingdom Trust made a measly offering of twelve (12) months of identity theft protection services to select Class Members.³¹ Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has *already occurred*.

48. All in all, Kingdom Trust failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

49. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

D. Cybercriminals Have and Will Use Plaintiffs' and the Class's Private Information to Defraud Them.

50. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

51. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.³²

52. For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of

³⁰ *Id.*

³¹ *See, e.g.*, Ex. 1.

³² *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

identity theft.³³ These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

53. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It’s hard to change your Social Security number and it’s not a good idea because it is connected to your life in so many ways.³⁴ (Emphasis added).

54. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.³⁵

55. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of breaching financial companies like Kingdom Trust is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

56. Indeed, a social security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.³⁶

57. “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”³⁷

³³ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

³⁴ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

³⁵ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at <https://www.gao.gov/products/gao-07-737>.

³⁶ Michael Kan, *Here’s How Much Your Identity Goes for on the Dark Web* (Nov. 15, 2017), <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

³⁷ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

58. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to PII, *they will use it*.³⁸

59. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n 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.³⁹

60. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.⁴⁰

61. With this Data Breach, identity thieves have already started to prey on the Kingdom Trust Data Breach victims, and we can anticipate that this will continue.

62. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.⁴¹

63. Defendant’s offer of one (1) year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures.

64. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is

³⁸ Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info_.

³⁹ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at <https://www.gao.gov/products/gao-07-737>.

⁴⁰ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

⁴¹ *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), available at <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

1 stolen and when it is used.

2 65. Once the twelve (12) months have expired, Plaintiffs and Class Members will need
3 to pay for their own identity theft protection and credit monitoring for the rest of their lives due
4 to Kingdom Trust's gross negligence.

5 66. Furthermore, identity monitoring only alerts someone to the fact that they have
6 *already been the victim of identity theft* (i.e., fraudulent acquisition and use of another person's
7 PII)—it does not prevent identity theft.⁴² Nor can an identity monitoring service remove Private
8 Information from the dark web.⁴³

9 67. "The people who trade in stolen personal information [on the dark web] won't
10 cooperate with an identity theft service or anyone else, so it's impossible to get the information
11 removed, stop its sale, or prevent someone who buys it from using it."⁴⁴

12 68. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have
13 been damaged and have been placed at an imminent, immediate, and continuing increased risk of
14 harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and
15 effort to mitigate the actual and potential impact of the Data Breach on their everyday lives,
16 including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial
17 institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank
18 accounts and credit reports for unauthorized activity for years to come.

19 69. Even more seriously is the identity restoration that Plaintiffs and other Class
20 Members must go through, which can include spending countless hours filing police reports,
21 filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle
22 driver's license replacement applications, and calling financial institutions to cancel fraudulent
23 credit applications, to name just a few of the steps Plaintiffs and the Class must take.

24 _____
25 ⁴² See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov.
26 30, 2017, 9:00 AM), <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

27 ⁴³ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar.
28 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.

⁴⁴ *Id.*

1 70. Plaintiffs and the Class have or will experience the following concrete and
2 particularized harms for which they are entitled to compensation, including:

- 3 a. Actual identity theft;
- 4 b. Trespass, damage to, and theft of their personal property including Private
5 Information;
- 6 c. Improper disclosure of their Private Information;
- 7 d. The imminent and certainly impending injury flowing from potential fraud and
8 identity theft posed by their Private Information being placed in the hands of
9 criminals;
- 10 e. Loss of privacy suffered as a result of the Data Breach, including the harm of
11 knowing cyber criminals have their Private Information;
- 12 f. Ascertainable losses in the form of time taken to respond to identity theft and
13 attempt to restore identity, including lost opportunities and lost wages from
14 uncompensated time off from work;
- 15 g. Ascertainable losses in the form of out-of-pocket expenses and the value of their
16 time reasonably expended to remedy or mitigate the effects of the Data Breach;
- 17 h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class
18 Members' Private Information for which there is a well-established and
19 quantifiable national and international market;
- 20 i. The loss of use of and access to their credit, accounts, and/or funds;
- 21 j. Damage to their credit due to fraudulent use of their Private Information; and/or
- 22 k. Increased cost of borrowing, insurance, deposits, and the inability to secure more
23 favorable interest rates because of a reduced credit score.

24 71. Moreover, Plaintiffs and Class Members have an interest in ensuring that their
25 Private Information, which remains in the possession of Defendant, is protected from further data
26 breaches by the implementation of industry standard security measures and safeguards. Defendant
27 has shown itself wholly incapable of protecting Plaintiffs' and the Class's Private Information.
28

72. Plaintiffs and Class Members also have an interest in ensuring that their Private Information that was provided to Kingdom Trust is removed from all Kingdom Trust servers, systems, and files.

73. Defendant itself acknowledged the harm caused by the Data Breach because it offered some Class Members woefully inadequate credit monitoring services. Twelve (12) months credit monitoring services is, however, inadequate to protect Plaintiffs and Class Members from the lifetime risk of identity theft and fraud they face.

74. Defendant further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur because it advised victims of the Data Breach to enroll in credit monitoring services, place a fraud alert/security freeze on credit files, and obtain a free credit report.⁴⁵

75. At Kingdom Trust's suggestion, Plaintiffs and the Class are desperately trying to mitigate the damage that Kingdom Trust has caused them.

76. Given the kind of Private Information Kingdom Trust made accessible to hackers, however, Plaintiffs and the Class are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.⁴⁶

77. None of this should have happened because the Data Breach was entirely preventable.

E. Defendant was Aware of the Risk of Data Breaches and SIM Swapping.

78. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some

⁴⁵ Exs. 1–2.

⁴⁶ *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

of the biggest data breaches, including Target,⁴⁷ Yahoo,⁴⁸ Marriott International,⁴⁹ Chipotle, Chili's, Arby's,⁵⁰ and others.⁵¹

79. Businesses in the financial services industry, such as Kingdom Trust, are prime targets for data breaches because they provide cybercriminals with maximum impact and maximum profit.⁵² Financial institutions, such as Defendant, store highly valuable data, and their digital transformation efforts create greater opportunities for threat actors to access that data.⁵³ This is why the financial sector is disproportionately targeted by cybercriminals, behind healthcare.⁵⁴

80. In fact, in 2023 the financial sector suffered the most data breaches.⁵⁵

81. The financial sector is an attractive target for cybercriminals not only for the immediate financial gain but also due to the wealth of sensitive customer information it holds.⁵⁶

82. SIM swapping has been on the rise in recent years. Washington National Insurance and Bankers Life, both subsidiaries of the CNO Financial Group, were targeted by SIM-swapping

⁴⁷ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.

⁴⁸ Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

⁴⁹ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/> (last visited Oct. 9, 2023).

⁵⁰ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b>.

⁵¹ See, e.g., Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

⁵² <https://www.upguard.com/blog/biggest-data-breaches-financial-services>.

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ <https://finance.yahoo.com/news/financial-industry-suffered-most-data-182214946.html>.

⁵⁶ *Id.*

hackers in November 2023.⁵⁷

83. Kingdom Trust should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the Private Information that it collected and maintained.

84. Kingdom Trust was aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

F. Kingdom Trust Could Have Prevented the SIM Swap.

85. SIM swaps, like the one that occurred at Kingdom Trust, are preventable. SIM swapping can be prevented by “using complex and unique passwords and keeping any personal information off of social media. SIM swaps prey on easy-to-guess passwords and private details in order to trick cell service carriers they are a paying customer. Authenticator apps like Google Authenticator and physical security keys like Yubikey also greatly increase SIM swap prevention.”⁵⁸

86. “Unlike what the name suggests, SIM swapping doesn’t require a cybercriminal to get access to your physical phone and steal your SIM card. SIM swapping can happen remotely. A hacker, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.”⁵⁹

87. “SIM swapping attacks pose a serious danger to business because they enable threat actors to gain access to corporate communications, accounts, and sensitive information like financial data.”⁶⁰ Thus, it is extremely important that businesses and their employees, such as

⁵⁷ <https://www.bitdefender.com/en-gb/blog/hotforsecurity/us-insurance-firms-sound-alarm-after-66-000-individuals-impacted-by-sim-swap-attack/>; *see also* <https://www.coalitioninc.com/blog/sim-swapping-extortion>.

⁵⁸ <https://www.avast.com/c-sim-swap-scam>.

⁵⁹ <https://www.mcafee.com/blogs/mobile-security/what-is-sim-swapping/>.

⁶⁰ https://usa.kaspersky.com/blog/what-is-sim-swapping/29868/?srsltid=AfmBOoqRaw_Ehw6APnL0jxdo2DqJltjZkqo_MTwHpPe11qx0vPAiLlsG.

Kingdom Trust, adequately protect itself from SIM swapping to protect the plethora of sensitive information they hold.

88. “Criminals increasingly target senior-level executives in an attack that can impact their corporate and home office environments and even extend to family members.”⁶¹

89. “Executives are attractive targets for cybercriminals. Their privileged access to a corporate network is inviting to cybercriminals looking to exploit valuable data, corporate networks or any means to extort large sums of money. Criminals may frequently target high-profile executives with a strong media/social media presence and/or those perceived to be involved in high-value transactions or negotiations. The company size and revenue can be a factor, as executives of these companies are more lucrative targets. Of course, with access to personal data and compromised credentials readily available on dark web marketplaces, the barrier to entry has become much lower and unsophisticated criminals can easily perpetrate these attacks.”⁶²

90. SIM swapping is preventable. Experian recommends the following measures to prevent SIM swapping:⁶³

- Try to use non-SMS multifactor authentication. Some accounts let you enable [multifactor authentication \(MFA\)](#) that doesn't rely on text messages. For example, you might be able to use an authenticator app, hardware token (a device that generates codes) or your fingerprint or face scan instead of a texted code. Then, even if someone takes over your number, they won't be able to get into your account or reset your password.
- Try to keep your personal information personal. The attackers will need to know personal details if they want to impersonate you when calling your carrier. Run a [free privacy scan](#) to see what's available online, and look into ways to [remove your information from people search sites](#).
- Don't post about your assets online. Talking about how much crypto or retirement savings you have online could make you a target.
- Beware of social engineering attacks. Fraudsters may try to trick you into sharing personal information that they can sell or use for a SIM swap. For example, they could pretend to be a customer representative who needs to verify your name, address and other personal information. Beware of these [phishing, smishing and vishing](#) attacks, which are sent via email, text or call, respectively.

⁶¹ <https://woodrufflawyer.com/insights/cyber-sim-swapping>.

⁶² *Id.*

⁶³ <https://www.experian.com/blogs/ask-experian/how-to-protect-yourself-from-sim-swapping/>.

91. Furthermore, McAfee recommends the following measures to prevent SIM swapping:⁶⁴

How to Prevent SIM Swapping

Check out these tips to keep your device and personal information safe from SIM swapping.

1. **Set up two-factor authentication using authentication apps.** Two-factor authentication is always a great idea; however, in the case of SIM swapping, the most secure way to access authentication codes is through authentication apps, versus emailed or texted codes. It's also a great idea to add additional security measures to authentication apps, such as protecting them with a PIN code, fingerprint, or face ID. Choose pin codes that are not associated with birthdays, anniversaries, or addresses. Opt for a random assortment of numbers.
2. **Watch out for phishing attempts.** Cybercriminals often gain fodder for their identity-thieving attempts through phishing. Phishing is a method cybercriminals use to fish for sensitive personal information that they can use to impersonate you or gain access to your financial accounts. Phishing emails, texts, and phone calls often use fear, excitement, or urgency to trick people into giving up valuable details, such as social security numbers, birthdays, passwords, and PINs. Be wary of messages from people and organizations you don't know. Even if the sender looks familiar, there could be typos in the sender's name, logo, and throughout the message that are a good tipoff that you should delete the message immediately. Never click on links in suspicious messages.
3. **Use a password manager.** Your internet browser likely asks you if you'd like the sites you visit to remember your password. Always say no! While password best practices can make it difficult to remember all your unique, long, and complex passwords and passphrases, do not set up autofill as a shortcut. Instead, entrust your passwords and phrases to a secure password manager, which is included in McAfee+. A secure password manager makes it so you only have to remember one password. The rest of them are encrypted and protected by two-factor authentication. A password manager makes it very difficult for a cybercriminal to gain entry to your accounts, thus keeping them safe.

92. Kingdom Trust should have required all employees and executives to use multi-factor authentication that *did not* rely on text messages and instead required employees and executives to use authentication apps to prevent the Breach.

93. "Relying solely on traditional authentication methods such as passwords or SMS codes can be risky, as it exposes you to SIM swapping attacks. Implementing a robust MFA solution that combines secure authentication via push notifications or QR codes, with an additional authentication factor based on the DNA of the mobile device, ensures that your employees or customers (in the case of MSPs) are protected. This additional protection ensures

⁶⁴ <https://www.mcafee.com/blogs/mobile-security/what-is-sim-swapping/>.

1 that even if an attacker manages to clone a user's device, they will not be able to access their
2 accounts because the DNA of the cloned device won't match and will be blocked.”⁶⁵

3 94. Kingdom Trust should have required all employees and executives to complete
4 training aimed at preventing social engineering attacks and phishing attempts to prevent the Data
5 Breach at issue.

6 95. Kingdom Trust should not have allowed employees and executives to store any
7 Kingdom Trust affiliated passwords, usernames, or other information on mobile device
8 applications or in internet browsers for easy login.

9 96. What is most alarming is that the perpetrator of the Breach was able to gain access
10 to Kingdom Trust's systems and networks after performing the SIM swap. This makes it apparent
11 that Kingdom Trust did not have sufficient data security in place. The perpetrator of the Breach
12 should not have been so easily able to gain access to Kingdom Trust's systems and networks.

13 97. In sum, there were many easy preventative measures Kingdom Trust could have
14 taken, or required its employees and executives to take, to prevent the Data Breach. However,
15 Kingdom Trust failed to implement any of the above measures. If Kingdom Trust had
16 implemented the above measures, the Data Breach would not have occurred.

17 98. “As SIM-swapping attacks continue to rise, executives must be vigilant and
18 proactive in safeguarding their personal and professional data.”⁶⁶

19 **G. Kingdom Trust Could Have Prevented the Data Breach.**

20 99. Data breaches are preventable.⁶⁷ As Lucy Thompson wrote in the DATA BREACH
21 AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have
22 been prevented by proper planning and the correct design and implementation of appropriate
23 security solutions.”⁶⁸ She added that “[o]rganizations that collect, use, store, and share sensitive
24

25 ⁶⁵ <https://www.watchguard.com/wgrd-news/blog/sim-swapping-ongoing-threat>.

26 ⁶⁶ <https://woodruffsawyer.com/insights/cyber-sim-swapping>.

27 ⁶⁷ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* DATA
BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at
<https://lawcat.berkeley.edu/record/394088>.

28 ⁶⁸ *Id.* at 17.

1 personal data must accept responsibility for protecting the information and ensuring that it is not
2 compromised”⁶⁹

3 100. “Most of the reported data breaches are a result of lax security and the failure to
4 create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information
5 security controls, including encryption, must be implemented and enforced in a rigorous and
6 disciplined manner so that a *data breach never occurs*.”⁷⁰

7 101. In a data breach like this, many failures laid the groundwork for the Breach.

8 102. The FTC has published guidelines that establish reasonable data security practices
9 for businesses.

10 103. The FTC guidelines emphasize the importance of having a data security plan,
11 regularly assessing risks to computer systems, and implementing safeguards to control such
12 risks.⁷¹

13 104. The FTC guidelines establish that businesses should protect the confidential
14 information that they keep; properly dispose of personal information that is no longer needed;
15 encrypt information stored on computer networks; understand their network’s vulnerabilities; and
16 implement policies for installing vendor-approved patches to correct security problems.

17 105. The FTC guidelines also recommend that businesses utilize an intrusion detection
18 system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating
19 hacking attempts; watch for large amounts of data being transmitted from the system; and have a
20 response plan ready in the event of a breach.

21 106. According to information and belief, Kingdom Trust failed to maintain many
22 reasonable and necessary industry standards necessary to prevent a data breach, including the
23 FTC’s guidelines.

24
25
26 ⁶⁹*Id.* at 28.

⁷⁰*Id.*

27 ⁷¹ *Protecting Personal Information: A Guide for Business*, FTC, available at
28 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

1 107. Upon information and belief, Kingdom Trust also failed to meet the minimum
2 standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special
3 Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program
4 (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which
5 are well respected authorities in reasonable cybersecurity readiness.

6 108. As explained by the Federal Bureau of Investigation, "[p]revention is the most
7 effective defense against ransomware and it is critical to take precautions for protection."⁷²

8 109. Defendant could and should have implemented, as recommended by the Federal
9 Bureau of Investigation, the following measures:

- 10 • Implement an awareness and training program. Because end users are targets,
11 employees and individuals should be aware of the threat of ransomware and
12 how it is delivered.
- 13 • Enable strong spam filters to prevent phishing emails from reaching the end
14 users and authenticate inbound email using technologies like Sender Policy
15 Framework (SPF), Domain Message Authentication Reporting and
16 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent
17 email spoofing.
- 18 • Scan all incoming and outgoing emails to detect threats and filter executable
19 files from reaching end users.
- 20 • Configure firewalls to block access to known malicious IP addresses.
- 21 • Patch operating systems, software, and firmware on devices. Consider using a
22 centralized patch management system.
- 23 • Set anti-virus and anti-malware programs to conduct regular scans
24 automatically.

25
26
27 ⁷² See How to Protect Your Networks from RANSOMWARE, at 3, available at
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁷³

110. Further, Kingdom Trust could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

⁷³ *Id.* at 3–4.

- 1 • **Update and patch your computer.** Ensure your applications and operating
2 systems (OSs) have been updated with the latest patches. Vulnerable
3 applications and OSs are the target of most ransomware attacks....
- 4 • **Use caution with links and when entering website addresses.** Be careful
5 when clicking directly on links in emails, even if the sender appears to be
6 someone you know. Attempt to independently verify website addresses (e.g.,
7 contact your organization's helpdesk, search the internet for the sender
8 organization's website or the topic mentioned in the email). Pay attention to
9 the website addresses you click on, as well as those you enter yourself.
10 Malicious website addresses often appear almost identical to legitimate sites,
11 often using a slight variation in spelling or a different domain (e.g., .com
12 instead of .net)....
- 13 • **Open email attachments with caution.** Be wary of opening email
14 attachments, even from senders you think you know, particularly when
15 attachments are compressed files or ZIP files.
- 16 • **Keep your personal information safe.** Check a website's security to ensure
17 the information you submit is encrypted before you provide it....
- 18 • **Verify email senders.** If you are unsure whether or not an email is legitimate,
19 try to verify the email's legitimacy by contacting the sender directly. Do not
20 click on any links in the email. If possible, use a previous (legitimate) email to
21 ensure the contact information you have for the sender is authentic before you
22 contact them.
- 23 • **Inform yourself.** Keep yourself informed about recent cybersecurity threats
24 and up to date on ransomware techniques. You can find information about
25 known phishing attacks on the Anti-Phishing Working Group website. You
26 may also want to sign up for CISA product notifications, which will alert you
27 when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been
28 published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....⁷⁴

111. In addition, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
 - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
 - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
 - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
 - Monitor for adversarial activities
 - Hunt for brute force attempts
 - Monitor for cleanup of Event Logs
 - Analyze logon events
- **Harden infrastructure**

⁷⁴ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://www.cisa.gov/news-events/news/protecting-against-ransomware>.

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁷⁵

112. Given that Kingdom Trust was storing the PII of thousands of individuals, Kingdom Trust could have and should have implemented all of the above measures to prevent and detect cyberattacks.

113. Specifically, among other failures, Kingdom Trust had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.⁷⁶

114. Moreover, it is a well-established industry standard practice for a business to dispose of confidential PII once it is no longer needed.

115. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁷⁷ Kingdom Trust, rather than following this basic standard of care, kept thousands of individuals’ unencrypted PII indefinitely.

116. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all PII.

117. Further, the scope of the Data Breach could have been dramatically reduced had Kingdom Trust utilized proper record retention and destruction practices.

⁷⁵ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

⁷⁶ See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

⁷⁷ *Protecting Personal Information: A Guide for Business*, FTC, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

H. Plaintiffs' Individual Experience

Plaintiff Kevin Meagher

118. Plaintiff Meagher received a Notice of Data Breach Letter from Defendant informing him that his highly confidential Private Information was compromised in the Data Breach.⁷⁸

119. Defendant was in possession of Plaintiff's Private Information before, during, and after the Data Breach.

120. Because of the Data Breach, there is no doubt Plaintiff Meagher's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had *accessed* Defendant's systems, but it confirmed that the unauthorized criminal actor may have *copied* files containing highly sensitive PII.⁷⁹ As such, Plaintiff Meagher and the Class are at an imminent risk of identity theft and fraud.

121. As a result of the Data Breach, Plaintiff Meagher has already expended **10 hours** of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements, credit reports, and/or other information. Additionally, Plaintiff has also placed a security freeze with two credit bureaus.

122. Plaintiff Meagher places significant value on the security of his Private Information and does not readily disclose it. Plaintiff Meagher has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

123. Plaintiff Meagher has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and

⁷⁸ Ex. 1.

⁷⁹ *Id.*

1 increased risk of future harm Plaintiff Meagher, and the Class now face by offering temporary,
2 non-automatic credit monitoring services to Plaintiff Meagher and the Class.

3 124. Knowing that thieves intentionally targeted and stole his Private Information,
4 including his Social Security number, and knowing that his Private Information is in the hands of
5 cybercriminals has caused Plaintiff Meagher great anxiety beyond mere worry. Specifically,
6 Plaintiff Meagher has lost hours of sleep, is in a constant state of stress, is very frustrated, and is
7 in a state of persistent worry now that his Private Information has been stolen.

8 125. Plaintiff Meagher has a continuing interest in ensuring that his Private Information,
9 which, upon information and belief, remains in the possession of Defendant, is protected, and
10 safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's
11 Private Information will be wholly unprotected and at-risk of future data breaches.

12 126. Plaintiff Meagher has suffered injuries directly and proximately caused by the Data
13 Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain
14 impending injury flowing from anticipated fraud and identity theft posed by his Private
15 Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value
16 of his Private Information that was entrusted to Defendant with the understanding that Defendant
17 would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with
18 Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between
19 what Plaintiff Meagher should have received from Defendant and Defendant's defective and
20 deficient performance of that obligation by failing to provide reasonable and adequate data
21 security and failing to protect his Private Information; and (v) continued risk to his Private
22 Information, which remains in the possession of Defendant and which is subject to further
23 breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the
24 Private Information that was entrusted to Defendant.

25 ***Plaintiff Rebecca Dawson***

26 127. Plaintiff Dawson received a Notice of Data Breach Letter from Defendant
27 informing her that her highly confidential Private Information was compromised in the Data
28

1 Breach.⁸⁰

2 128. Defendant was in possession of Plaintiff's Private Information before, during, and
3 after the Data Breach. Plaintiff Dawson's Private Information, including her Social Security
4 number, were provided to Defendant in connection with an SBA loan Plaintiff Dawson applied
5 for.

6 129. Because of the Data Breach, there is no doubt Plaintiff Dawson's highly
7 confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of
8 Data Breach Letter from Defendant not only disclosed that an unauthorized third-party had
9 *accessed* Defendant's systems, but it confirmed that the unauthorized criminal actor may have
10 *copied* files containing highly sensitive PII.⁸¹ As such, Plaintiff Dawson and the Class are at an
11 imminent risk of identity theft and fraud.

12 130. As a result of the Data Breach, Plaintiff Dawson has already expended over **100**
13 **hours** of her time and has suffered loss of productivity from taking time to address and attempt
14 to ameliorate, mitigate, and address the future consequences of the Data Breach, including
15 investigating the Data Breach, investigating how best to ensure that she is protected from identity
16 theft, mitigating the fraud and identity theft that has already occurred, signing up for credit
17 monitoring services, and reviewing account statements, credit cards statements, credit reports,
18 and/or other information.

19 131. As a result of the Data Breach, Plaintiff Dawson has already experienced
20 significant identity theft and fraud.

- 21 a. On or around July 24, 2024, through July 25, 2024, Plaintiff Dawson became the
22 victim of an unauthorized SIM swap. After the cybercriminal successfully initiated
23 the SIM swap, the perpetrator was able to access Plaintiff Dawson's AOL email
24 account and re-routed all her emails from Experian, Wells Fargo, Spectrum, Chase,
25 and Bank of America into an archive folder so that Plaintiff could not see or readily
26

27

⁸⁰ Ex. 2.

28 ⁸¹ *Id.*

1 determine how the perpetrator was misusing her Private Information.

2 b. On or around August 10, 2024, through August 13, 2024, Plaintiff lost access to
3 her Wells Fargo online banking due to fraud. On August 13, 2024, Plaintiff was
4 informed by Wells Fargo that there was fraudulent activity on her account, which
5 was why her online banking access was denied. Once Plaintiff Dawson was able
6 to access her online account with Wells Fargo, she discovered the following
7 fraudulent activity:

8 i. On July 24, 2024, a Vector Space LLV wire of \$5,100.00 was declined by
9 Wells Fargo; and

10 ii. On July 24, 2024, there were five (5) separate Zelle transactions totaling
11 \$1,000.

12 c. On or around July 26, 2024, an ACH transaction of \$2,500.00 was transferred out
13 of Plaintiff Dawson's Wells Fargo Checking account to an Experian Smart Money
14 account. The Experian Smart Money account was not set up by Plaintiff Dawson
15 but was opened utilizing all of Plaintiff Dawson's personal information.

16 d. As a result of the extensive fraud and identity theft Plaintiff Dawson experienced,
17 Plaintiff Dawson filed a police report with the West Los Angeles Police
18 Department.

19 132. The fraud and identity theft Plaintiff Dawson experienced is directly traceable to
20 the Data Breach. The information exposed in the Data Breach gave cybercriminals all the
21 information they needed to initiate a SIM swap on Plaintiff Dawson's cellphone. Hackers often
22 persuade mobile phone carriers to perform a SIM swap by using personal information leaked in a
23 data breach—such as the one at issue here.⁸² Once the hacker took control of Plaintiff Dawson's
24 cellphone, this allowed the cybercriminals to further exploit Plaintiff Dawson by accessing her
25 email account, bank account, and text messages.

26 133. Due to the Data Breach and the identity theft and fraud Plaintiff has already
27

28 ⁸² <https://staysafeonline.org/resources/sim-card-swap-scams/>.

1 experienced, Plaintiff purchased Aura credit monitoring services for \$168.00.

2 134. In addition to the Breach exposing all the information needed for a cybercriminal
3 to perform a SIM swap, Kingdom Trust was also in possession of Plaintiff's Social Security
4 number at the time of the Breach. Oftentimes, cybercriminals will compile information from
5 multiple data breaches to create a "fullz package" (a full set of personal information).⁸³ Indeed,
6 "[c]yber criminals are focused on bringing together an individual's full information to facilitate
7 identity theft, allow the purchase of goods and services on the Internet, and enable criminals to
8 open new accounts in a victim's name. Fullz are also for sale in underground markets and the dark
9 web, ranging in price from \$15 to \$65 for a U.S. citizen's complete record... Like a business
10 building a profile of a customer, criminals are trying to create a complete digital dossier on
11 potential victims."⁸⁴ "The common assumption is that if a hacker doesn't intercept highly
12 sensitive information—such as your Social Security number or a credit card number—and instead
13 gets hold of other personally identifiable information, you'll probably be fine. This assumption is
14 simply false...Starting with a single piece of PII, whether sensitive or not, a threat actor can begin
15 to piece together the puzzle. The journey to identity theft begins with that single step."⁸⁵

16 135. Plaintiff Dawson also experienced spam texts shortly after the Data Breach, which
17 is certainly not a coincidence since Kingdom Trust admits it breached her mobile number.⁸⁶

18 136. Plaintiff Dawson places significant value on the security of her Private Information
19 and does not readily disclose it. Plaintiff Dawson has never knowingly transmitted unencrypted
20 Private Information over the internet or any other unsecured source. Plaintiff also does not share
21 personal information online.

22
23 ⁸³ <https://www.pcworld.com/article/414992/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html>.

24 ⁸⁴ *Id.*; see also <https://www.csoonline.com/article/570759/how-cybercriminals-turn-harmless-stolen-or-leaked-data-into-dollars.html> ("Threat actors have become sophisticated in how they
25 treat stolen data. They're taking any new data they get and merging it with data they already have
26 to grow their databases. In one dataset, they might have a first name and last name. In another, a
first name, last name and email address.").

27 ⁸⁵ <https://www.csoonline.com/article/570759/how-cybercriminals-turn-harmless-stolen-or-leaked-data-into-dollars.html>.

28 ⁸⁶ Ex. 2.

1 137. Plaintiff Dawson has been and will continue to be at a heightened and substantial
2 risk of future identity theft and its attendant damages for years to come. Such a risk is certainly
3 real and impending, and is not speculative, given the highly sensitive nature of the Private
4 Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and
5 increased risk of future harm Plaintiff Dawson, and the Class now face by offering temporary,
6 non-automatic credit monitoring services to certain members of the Class.

7 138. Knowing that thieves intentionally targeted and stole her Private Information and
8 knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff
9 Dawson great anxiety beyond mere worry. Specifically, Plaintiff Dawson has lost hours of sleep,
10 is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that her
11 Private Information has been stolen.

12 139. Plaintiff Dawson has a continuing interest in ensuring that her Private Information,
13 which, upon information and belief, remains in the possession of Defendant, is protected, and
14 safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's
15 Private Information will be wholly unprotected and at-risk of future data breaches.

16 140. Plaintiff Dawson has suffered injuries directly and proximately caused by the Data
17 Breach, including: (i) theft and misuse of her valuable Private Information; (ii) the imminent and
18 certain impending injury flowing from anticipated fraud and identity theft posed by her Private
19 Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value
20 of her Private Information that was entrusted to Defendant with the understanding that Defendant
21 would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with
22 Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between
23 what Plaintiff Dawson should have received from Defendant and Defendant's defective and
24 deficient performance of that obligation by failing to provide reasonable and adequate data
25 security and failing to protect her Private Information; and (v) continued risk to her Private
26 Information, which remains in the possession of Defendant and which is subject to further
27 breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the
28 Private Information that was entrusted to Defendant.

V. **CLASS ACTION ALLEGATIONS**

141. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

142. Plaintiffs bring this action against Kingdom Trust on behalf of themselves and on behalf of all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of the following Nationwide Class (“Class”) and California Subclass:

Nationwide Class:

All persons who were sent a Notice of Data Breach Letter from Kingdom Trust in response to the Data Breach.

California Subclass:

All persons residing in California who were sent a Notice of Data Breach Letter from Kingdom Trust after the Data Breach.

143. Excluded from the Class(es) are Defendant, any entity in which Defendant has a controlling interest, and Defendant’s officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

144. Plaintiffs reserve the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

145. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class(es). Upon information and belief, Defendant’s own business records or electronic media can be utilized for the notice process.

146. The proposed Class and Subclass meet the requirements of Federal Rule of Civil Procedure 23.

147. **Numerosity:** The proposed Class(es) are so numerous that joinder of all members is impracticable. The Class(es) are comprised of over 30,000 people.

1 148. **Typicality:** Plaintiffs' claims are typical of the claims of the Class(es). Plaintiffs
2 and all members of the Class(es) were injured through Kingdom Trust's uniform misconduct.
3 Kingdom Trust's inadequate data security gave rise to Plaintiffs' claims and are identical to those
4 that give rise to the claims of every other Class Member because Plaintiffs and each member of
5 the Class(es) had their sensitive Private Information compromised in the same way by the same
6 conduct of Kingdom Trust.

7 149. **Adequacy:** Plaintiffs are adequate representatives of the Class(es) because
8 Plaintiffs' interests do not conflict with the interests of the Class(es); Plaintiffs have retained
9 counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and
10 Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class(es) will
11 be fairly and adequately protected by Plaintiffs and their counsel.

12 150. **Superiority:** A class action is superior to other available means of fair and
13 efficient adjudication of the claims of Plaintiffs and the Class(es). The injury suffered by each
14 individual Class Member is relatively small in comparison to the burden and expense of individual
15 prosecution of complex and expensive litigation. It would be very difficult if not impossible for
16 members of the Class(es) to individually and effectively redress Kingdom Trust's wrongdoing.
17 Even if Class Members could afford such individual litigation, the court system could not.
18 Individualized litigation presents a potential for inconsistent or contradictory judgments.
19 Individualized litigation increases the delay and expense to all parties, and to the court system,
20 presented by the complex legal and factual issues of the case. By contrast, the class action device
21 presents far fewer management difficulties and provides benefits of single adjudication, economy
22 of scale, and comprehensive supervision by a single court.

23 151. **Commonality and Predominance:** There are many questions of law and fact
24 common to the claims of Plaintiffs and the other members of the Class(es), and those questions
25 predominate over any questions that may affect individual members of the Class(es). Common
26 questions for the Class include:

- 27 a. Whether Defendant engaged in the wrongful conduct alleged herein;
28

- b. Whether Defendant failed to adequately safeguard Plaintiffs' and Class Members' Private Information;
- c. Whether Defendant owed a duty to Plaintiffs and Class Members to adequately protect their Private Information, and whether it breached this duty;
- d. Whether Kingdom Trust breached its duties to Plaintiffs and Class Members;
- e. Whether Kingdom Trust failed to provide adequate data security, procedures and protocols;
- f. Whether Kingdom Trust knew or should have known that its network and/or employees and executives were vulnerable to SIM swapping;
- g. Whether Kingdom Trust had data security measures, policies, and procedures in place to prevent SIM swapping;
- h. Whether Kingdom Trust's conduct, including its failure to act, resulted in or was the proximate cause of the Breach of its company network;
- i. Whether Kingdom Trust was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within its network;
- j. Whether Kingdom Trust was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;
- k. Whether Kingdom Trust breached implied contractual duties to Plaintiffs and Class Members to use reasonable care in protecting their Private Information;
- l. Whether Kingdom Trust failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;
- m. Whether Kingdom Trust continues to breach duties to Plaintiffs and Class Members;
- n. Whether Plaintiffs and Class Members suffered injury as a proximate result of Kingdom Trust's negligent actions or failures to act;

o. Whether Plaintiffs and Class Members are entitled to recover damages, equitable relief, and other relief; and

p. Whether Kingdom Trust's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE

(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)

152. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

153. Defendant Kingdom Trust solicited, gathered, and stored the Private Information of Plaintiffs and the Class.

154. Defendant had full knowledge of the sensitivity of the Private Information it maintained and of the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendant had a duty to Plaintiffs and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiffs and the Class Members were the foreseeable victims of any inadequate data safety and security practices. Plaintiffs and the Class Members had no ability to protect their Private Information that was in Kingdom Trust's possession. As such, a special relationship existed between Kingdom Trust and Plaintiffs and the Class.

155. Kingdom Trust was well aware of the fact that cybercriminals routinely target corporations, particularly those in the financial industry, through data breaches and SIM swapping in an attempt to steal the Private Information it collects.

156. Defendant owed Plaintiffs and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

157. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of

foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

158. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to data breaches and SIM swapping. Some of the duties that Kingdom Trust owed Plaintiffs, and the Class include:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
- b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. To adequately and properly audit and test its systems;
- d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
- e. To train its employees not to store Private Information for longer than absolutely necessary;
- f. To train its employees about preventing SIM swapping;
- g. To implement processes to quickly detect a data breach, security incident, SIM swapping, or intrusion; and
- h. To promptly and timely notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

159. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect Private Information.

160. Plaintiffs and Class Members are consumers under the FTC Act.

1 161. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures
2 to protect Private Information and by not complying with industry standards. Accordingly,
3 Defendant has committed negligence *per se* by violating the FTC Act.

4 162. Various FTC publications and data security breach orders further form the basis of
5 Defendant's duty.

6 163. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties,
7 creating a special relationship between them and Kingdom Trust. Defendant was in a position to
8 ensure that its systems and employees were sufficient to protect the Private Information that
9 Plaintiffs and the Class entrusted to it.

10 164. Defendant breached its duties of care by failing to adequately protect Plaintiffs'
11 and Class Members' Private Information. Defendant breached its duties by, among other things:

- 12 a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding,
13 deleting, and protecting the Private Information in its possession;
- 14 b. Failing to protect the Private Information in its possession using reasonable and
15 adequate security procedures and systems;
- 16 c. Failing to adequately and properly audit and test its computer systems to avoid
17 data breaches and SIM swapping;
- 18 d. Failing to educate and train employees to prevent SIM swapping;
- 19 e. Failing to have data infrastructure, processes and systems in place to prevent harm
20 caused by SIM swapping;
- 21 f. Failing to adequately and properly audit, test, and train its employees regarding
22 how to properly and securely transmit and store Private Information, including
23 maintaining it in an encrypted format;
- 24 g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and
25 the Class's Private Information;
- 26 h. Failing to implement processes to quickly detect data breaches, security incidents,
27 SIM swapping, or intrusions;
- 28 i. Failing to abide by reasonable retention and destruction policies for Private

Information it collects and stores; and

- j. Failing to promptly and accurately notify Plaintiffs and Class Members of the Data Breach that exposed their Private Information.

165. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

166. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

167. The damages Plaintiffs and the Class have suffered (as alleged above) were and are reasonably foreseeable.

168. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

169. Plaintiffs and the Class have suffered injury, including as described herein, and are entitled to actual and punitive damages in an amount to be proven at trial.

**SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

170. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

171. Plaintiffs allege this claim in the alternative to their unjust enrichment claim and breach of third-party beneficiary contract claim.

172. Defendant acquired and maintained the Private Information of Plaintiffs and the Class including their Social Security numbers and other sensitive information to provide services.

173. In exchange, Defendant entered into implied contracts with Plaintiffs and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' Private Information and timely notify them of a Data Breach.

174. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards and measures

1 intended to prevent SIM swapping.

2 175. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and
3 Class Members' Private Information and failing to provide them with timely and accurate notice
4 of the Data Breach. Indeed, it took Defendant months to warn Plaintiffs and Class Member of
5 their imminent risk of identity theft.

6 176. As a direct and proximate result of Defendant's breach of implied contract,
7 Plaintiffs and Class Members have suffered damages, including foreseeable consequential
8 damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private
9 Information.

10 177. Plaintiffs and the Class have suffered injuries as described herein, and are entitled
11 to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in
12 an amount to be proven at trial.

13 **THIRD CAUSE OF ACTION**

14 **BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**

15 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

16 178. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

17 179. Plaintiffs allege this claim in the alternative to their unjust enrichment claim and
18 breach of implied contract claim.

19 180. On information and belief, Defendant entered into written contracts to provide
20 financial services to companies.

21 181. In exchange, Defendant agreed, in part, to implement adequate security measures
22 to safeguard the Private Information of Plaintiffs and the Class and to timely and adequately notify
23 them of the Data Breach.

24 182. According to information and belief, these contracts were made expressly for the
25 benefit of Plaintiffs and the Class, as Plaintiffs and Class Members were the intended third-party
26 beneficiaries of the contracts entered into between Defendant and its clients. Defendant knew that,
27 if it were to breach these contracts with its clients, Plaintiffs and Class Members would be harmed.

28 183. Defendant breached the contracts entered into with its clients by, among other

things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiffs and Class Members of the Data Breach.

184. Plaintiffs and the Class were harmed by Defendant's breaches of contract, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

185. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

**FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

186. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

187. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, (i) to act primarily for Plaintiffs and Class Members, (ii) for the safeguarding of their Private Information; (iii) to timely notify Plaintiffs and Class Members of a data breach's occurrence and disclosure; and (iv) to maintain complete and accurate records of what information (and where) Defendant did and does store.

188. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with Plaintiffs and the Class, in particular, to keep secure their Private Information.

189. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiffs and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

190. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing

1 to diligently discover, investigate, and give notice of the Data Breach in a reasonable and
2 practicable period of time.

3 191. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing
4 to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class
5 Members' Private Information.

6 192. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by
7 failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

8 193. Defendant breached its fiduciary duties to Plaintiffs and Class Members by
9 otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

10 194. As a direct and proximate result of Defendant's breaches of its fiduciary duties,
11 Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i)
12 invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private
13 Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual
14 consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs
15 associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory
16 damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their
17 Private Information, which: (a) remains unencrypted and available for unauthorized third parties
18 to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further
19 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
20 measures to protect the Private Information.

21 **FIFTH CAUSE OF ACTION**

22 **UNJUST ENRICHMENT**

23 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

24 195. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

25 196. Plaintiffs allege this claim in the alternative to their breach of contract claim(s).

26 197. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and
27 accepted and retained that benefit by accepting and retaining the Private Information entrusted to
28 it. Defendant profited from Plaintiffs' retained data and commercialized and used Plaintiffs' and

1 Class Members' Private Information for business purposes.

2 198. Upon information and belief, Defendant funds its data security measures entirely
3 from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class
4 Members.

5 199. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs
6 and Class Members is to be used to provide a reasonable level of data security, and the amount of
7 the portion of each payment made that is allocated to data security is known to Defendant.

8 200. Defendant failed to secure Plaintiffs' and Class Members' Private Information and,
9 therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private
10 Information provided.

11 201. Defendant acquired the Private Information through inequitable means as it failed
12 to disclose the inadequate data security practices previously alleged. If Plaintiffs and Class
13 Members had known that Defendant would not fund adequate data security practices, procedures,
14 and protocols to sufficiently monitor, supervise, and secure their Private Information, they would
15 not have entrusted their Private Information to Defendant or obtained services from Defendant's
16 clients.

17 202. Defendant enriched itself by saving the costs it reasonably should have expended
18 on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead
19 of providing a reasonable level of security that would have prevented the Data Breach, Defendant
20 instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by
21 utilizing cheaper, ineffective security measures and diverting those funds to their own benefit.
22 Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of
23 Defendant's decision to prioritize its own profits over the requisite security and the safety of their
24 Private Information.

25 203. Plaintiffs and Class Members have no adequate remedy at law.

26 204. Under the circumstances, it would be unjust for Defendant to be permitted to retain
27 any of the benefits that Plaintiffs and Class Members conferred upon it.

28 205. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class

Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiffs' efforts to prevent from succeeding.

206. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

SIXTH CAUSE OF ACTION
California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff Dawson and the California Subclass)

207. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

208. This claim is alleged on behalf of Plaintiff Dawson (referred to as "Plaintiff" throughout this claim) and on behalf of the California Subclass (referred to as "Class Members" throughout this claim).

209. Defendant's acts and omissions as alleged herein emanated and were directed from California.

210. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq.*

211. Defendant stored the Private Information of Plaintiff Dawson and Class Members in its computer systems.

212. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff Dawson's and Class Members' Private Information secure and prevented the loss or misuse of that Private Information.

213. Defendant did not disclose at any time that Plaintiff Dawson's and Class Members' Private Information was vulnerable to hackers because Defendant's data security measures and employee training were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

214. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its systems, specifically the security thereof, and its ability to safely store Plaintiffs' and Class Members' Private Information.

215. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures and employee training or follow industry standards for data security.

216. If Defendant had complied with these legal requirements, Plaintiff Dawson and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiffs and Class Members of the Data Breach.

217. Defendant's acts and omissions as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

218. Plaintiff Dawson and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff Dawson's and Class Members' Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff Dawson and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

219. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All these actions and omissions were clearly injurious to Plaintiff Dawson and Class Members, directly causing the harms alleged below.

220. Defendant engaged in unfair business practices under the "tethering test."

1 Defendant's actions and omissions, as described in detail above, violated fundamental public
2 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The
3 Legislature declares that . . . all individuals have a right of privacy in information pertaining to
4 them The increasing use of computers . . . has greatly magnified the potential risk to
5 individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code
6 § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about
7 California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the
8 Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide
9 concern."). Defendant's acts and omissions thus amount to a violation of the law.

10 221. Defendant engaged in unfair business practices under the "FTC test." The harm
11 caused by Defendant's actions and omissions, as described in detail above, is substantial in that it
12 affects thousands of Class Members and has caused those persons to suffer actual harm. Such
13 harms include a substantial risk of identity theft, disclosure of Plaintiff Dawson's and Class
14 Members' Private Information to third parties without their consent, diminution in value of their
15 Private Information, consequential out of pocket losses for procuring credit freeze or protection
16 services, identity theft monitoring, and other expenses relating to identity theft losses or protective
17 measures. This harm continues given the fact that Plaintiff Dawson's and Class Members' Private
18 Information remains in Defendant's possession, without adequate protection, and is also in the
19 hands of those who obtained it without their consent. Defendant's actions and omissions violated
20 Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts
21 or practices" as those that "cause[] or [are] likely to cause substantial injury to consumers which
22 [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing
23 benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No.
24 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate
25 measures to secure personal information collected violated §5(a) of FTC Act).

26 222. Plaintiff Dawson and Class Members suffered injury in fact and lost money or
27 property as the result of Defendant's unfair business practices. Plaintiff Dawson's and Class
28 Members' Private Information was taken and in the hands of those who will use it for their own

1 advantage, or is being sold for value, making it clear that the hacked information is of tangible
 2 value. Plaintiff Dawson's and Class Members have also suffered consequential out-of-pocket
 3 losses for procuring credit freeze or protection services, identity theft monitoring, and other
 4 expenses relating to identity theft losses or protective measures.

5 223. As a result of Defendant's unlawful and unfair business practices in violation of
 6 the UCL, Plaintiff Dawson and Class Members are entitled to damages, injunctive relief, and
 7 reasonable attorneys' fees and costs.

8 **SEVENTH CAUSE OF ACTION**
 9 **Violation of the California Consumer Privacy Act**
 10 **Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)**
(On Behalf of Plaintiff Dawson and the California Subclass)

11 224. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

12 225. This claim is alleged on behalf of Plaintiff Dawson (referred to as "Plaintiff"
 13 throughout this claim) and on behalf of the California Subclass (referred to as "California Subclass
 14 Members" throughout this claim).

15 226. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a),
 16 creates a private cause of action for violations of the CCPA.

17 227. Section 1798.150(a) specifically provides:

18 Any consumer whose nonencrypted and nonredacted personal information, as
 19 defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section
 20 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure
 21 as a result of the business's violation of the duty to implement and maintain
 22 reasonable security procedures and practices appropriate to the nature of the
 23 information to protect the personal information may institute a civil action for any
 24 of the following

- 25 i. To recover damages in an amount not less than one
 26 hundred dollars (\$100) and not greater than seven
 27 hundred and fifty (\$750) per consumer per incident or
 28 actual damages, whichever is greater.
- ii. Injunctive or declaratory relief.
- iii. Any other relief the court deems proper.

27 228. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized
 28 for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of

1 \$25 million.

2 229. Plaintiff and California Subclass Members are covered “consumers” under §
3 1798.140(g) in that they are natural persons who are California residents.

4 230. The personal information of Plaintiff and the California Subclass Members at issue
5 in this lawsuit constitutes “personal information” under § 1798.150(a) and 1798.81.5, in that the
6 personal information Defendant collects and which was impacted by the cybersecurity attack
7 includes an individual’s first name or first initial and the individual’s last name in combination
8 with one or more of the following data elements, with either the name or the data elements not
9 encrypted or redacted: (i) Social Security number; (ii) Driver’s license number, California
10 identification card number, tax identification number, passport number, military identification
11 number, or other unique identification number issued on a government document commonly used
12 to verify the identity of a specific individual; (iii) account number or credit or debit card number,
13 in combination with any required security code, access code, or password that would permit
14 access to an individual’s financial account; (iv) medical information; (v) health insurance
15 information; (vi) unique biometric data generated from measurements or technical analysis of
16 human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a
17 specific individual.

18 231. Defendant knew or should have known that its computer systems and data security
19 practices were inadequate to safeguard the California Subclass Members’ personal information
20 and that the risk of a data breach or theft was highly likely. Defendant failed to implement and
21 maintain reasonable security procedures and practices appropriate to the nature of the information
22 to protect the personal information of Plaintiff and the California Subclass Members. Specifically,
23 Defendant subjected Plaintiff’s and the California Subclass Members’ nonencrypted and
24 nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure
25 as a result of the Defendant’s violation of the duty to implement and maintain reasonable security
26 procedures and practices appropriate to the nature of the information, as described herein.

27 232. As a direct and proximate result of Defendant’s violation of its duty, the
28 unauthorized access and exfiltration, theft, or disclosure of Plaintiff’s and California Subclass

Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

233. As a direct and proximate result of Defendant's acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of Plaintiff's and California Subclass Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

234. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

235. Accordingly, Plaintiff and the California Subclass Members by way of this complaint seek actual pecuniary damages suffered as a result of Defendant's violations described herein.

236. Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant fails to respond or has not cured or is unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars (\$750) per consumer per incident. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

EIGHTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code §§ 1798.80 *et seq.*
(On Behalf of Plaintiff Dawson and the California Subclass)

237. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

238. This claim is alleged on behalf of Plaintiff Dawson (referred to as "Plaintiff" throughout this claim) and on behalf of the California Subclass (referred to as "California Subclass Members" throughout this claim).

239. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose

1 of this section is to encourage businesses that own, license, or maintain personal information about
2 Californians to provide reasonable security for that information.”

3 240. Section 1798.81.5(b) further states that: “[a] business that owns, licenses, or
4 maintains personal information about a California resident shall implement and maintain
5 reasonable security procedures and practices appropriate to the nature of the information, to
6 protect the personal information from unauthorized access, destruction, use, modification, or
7 disclosure.”

8 241. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of
9 this title may institute a civil action to recover damages.” Section 1798.84(e) further provides that
10 “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.”

11 242. Plaintiff and the California Subclass Members are “customers” within the meaning
12 of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal
13 information to Defendant for the purpose of obtaining a product and/or service from Defendant.

14 243. The personal information of Plaintiff and the California Subclass Members at issue
15 in this lawsuit constitutes “personal information” under § 1798.81.5(d)(1) in that the personal
16 information Defendant collects and which was impacted by the Data Breach includes an
17 individual’s first name or first initial and the individual’s last name in combination with one or
18 more of the following data elements, with either the name or the data elements not encrypted or
19 redacted: (i) Social Security number; (ii) Driver’s license number, California identification card
20 number, tax identification number, passport number, military identification number, or other
21 unique identification number issued on a government document commonly used to verify the
22 identity of a specific individual; (iii) account number or credit or debit card number, in
23 combination with any required security code, access code, or password that would permit access
24 to an individual’s financial account; (iv) medical information; (v) health insurance information;
25 (vi) unique biometric data generated from measurements or technical analysis of human body
26 characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific
27 individual.

28 244. Defendant knew or should have known that its computer systems and data security

1 practices were inadequate to safeguard the Plaintiff's and California Subclass Members' personal
2 information and that the risk of a data breach or theft was highly likely. Defendant failed to
3 implement and maintain reasonable security procedures and practices appropriate to the nature of
4 the information to protect the personal information of Plaintiff and the California Subclass
5 Members. Specifically, Defendant failed to implement and maintain reasonable security
6 procedures and practices appropriate to the nature of the information, to protect the personal
7 information of Plaintiff and the California Subclass Members from unauthorized access,
8 destruction, use, modification, SIM swapping, or disclosure. Defendant further subjected
9 Plaintiff's and the California Subclass Members' nonencrypted and nonredacted personal
10 information to an unauthorized access and exfiltration, theft, or disclosure as a result of the
11 Defendant's violation of the duty to implement and maintain reasonable security procedures and
12 practices appropriate to the nature of the information, as described herein.

13 245. As a direct and proximate result of Defendant's violation of its duty, the
14 unauthorized access, destruction, use, modification, or disclosure of the personal information of
15 Plaintiff and the California Subclass Members included hackers' access to, removal, deletion,
16 destruction, use, modification, disabling, disclosure and/or conversion of the personal information
17 of Plaintiff and the California Subclass Members by the cybercriminals and/or additional
18 unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the
19 information.

20 246. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the
21 California Subclass Members were injured and lost money or property including, but not limited
22 to, the loss of Plaintiff's and the California Subclass Members' legally protected interest in the
23 confidentiality and privacy of their personal information, nominal damages, and additional losses
24 described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to
25 Cal. Civ. Code § 1798.84(b).

26 247. Moreover, the California Customer Records Act further provides: "A person or
27 business that maintains computerized data that includes personal information that the person or
28 business does not own shall notify the owner or licensee of the information of the breach of the

1 security of the data immediately following discovery, if the personal information was, or is
2 reasonably believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82.

3 248. Any person or business that is required to issue a security breach notification under
4 the CRA must meet the following requirements under §1798.82(d):

- 5 a. The name and contact information of the reporting person or business subject to
6 this section;
- 7 b. A list of the types of personal information that were or are reasonably believed to
8 have been the subject of a breach;
- 9 c. If the information is possible to determine at the time the notice is provided, then
10 any of the following: (i) the date of the breach, (ii) the estimated date of the breach,
11 or (iii) the date range within which the breach occurred. The notification shall also
12 include the date of the notice;
- 13 d. Whether notification was delayed as a result of a law enforcement investigation, if
14 that information is possible to determine at the time the notice is provided;
- 15 e. A general description of the breach incident, if that information is possible to
16 determine at the time the notice is provided;
- 17 f. The toll-free telephone numbers and addresses of the major credit reporting
18 agencies if the breach exposed a social security number or a driver’s license or
19 California identification card number;
- 20 g. If the person or business providing the notification was the source of the breach,
21 an offer to provide appropriate identity theft prevention and mitigation services, if
22 any, shall be provided at no cost to the affected person for not less than 12 months
23 along with all information necessary to take advantage of the offer to any person
24 whose information was or may have been breached if the breach exposed or may
25 have exposed personal information.

26 249. Defendant failed to provide the legally compliant notice under § 1798.82(d) to
27 Plaintiff and members of the California Subclass. On information and belief, to date, Defendant
28 has not sent written notice of the data breach to all impacted individuals. As a result, Defendant

1 has violated § 1798.82 by not providing legally compliant and timely notice to all California
2 Subclass Members. Because not all members of the class have been notified of the breach,
3 members could have taken action to protect their personal information but were unable to do so
4 because they were not timely notified of the breach.

5 250. According to information and belief, many California Subclass Members affected
6 by the Breach have not received any notice at all from Defendant in violation of Section
7 1798.82(d).

8 251. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and California
9 Subclass Members suffered incrementally increased damages separate and distinct from those
10 simply caused by the breaches themselves.

11 252. As a direct consequence of the actions as identified above, Plaintiff and California
12 Subclass Members incurred additional losses and suffered further harm to their privacy, including
13 but not limited to economic loss, the loss of control over the use of their identity, increased stress,
14 fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the
15 investigation of the breach and effort to cure any resulting harm, the need for future expenses and
16 time dedicated to the recovery and protection of further loss, and privacy injuries associated with
17 having their sensitive personal information disclosed, that they would not have otherwise
18 incurred, and are entitled to recover compensatory damages according to proof pursuant to §
19 1798.84(b).

20 **NINTH CAUSE OF ACTION**
21 **DECLARATORY AND INJUNCTIVE RELIEF**
22 **(On Behalf of Plaintiffs, the Nationwide Class, and the California Subclass)**

23 253. Plaintiffs incorporate paragraphs 1–151 as though fully set forth herein.

24 254. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C.
25 § 2201.

26 255. As previously alleged, Plaintiffs and members of the Class are entered into implied
27 contracts with Defendant, which contracts required Defendant to provide adequate security for
28 the Private Information collected from Plaintiffs and the Class.

1 256. Defendant owed and still owes a duty of care to Plaintiffs and Class members that
2 require it to adequately secure Plaintiffs' and Class members' Private Information.

3 257. Upon reason and belief, Defendant still possesses the Private Information of
4 Plaintiffs and the Class members.

5 258. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs
6 and the Class members.

7 259. Since the Data Breach, Defendant has not yet announced any changes to its data
8 security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems
9 and/or security practices which permitted the Data Breach to occur and go undetected and,
10 thereby, prevent further attacks.

11 260. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs
12 and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the
13 Private Information in Defendant's possession is even more vulnerable to cyberattack.

14 261. Actual harm has arisen in the wake of the Data Breach regarding Defendant's
15 contractual obligations and duties of care to provide security measures to Plaintiffs and the
16 members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or
17 further harm due to the exposure of their Private Information and Defendant's failure to address
18 the security failings that led to such exposure.

19 262. There is no reason to believe that Defendant's security measures are any more
20 adequate now than they were before the Data Breach to meet Defendant's contractual obligations
21 and legal duties.

22 263. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing
23 security measures do not comply with its contractual obligations and duties of care to provide
24 adequate security, and (2) that to comply with its contractual obligations and duties of care,
25 Defendant must implement and maintain reasonable security measures, including, but not limited
26 to:

- 27 i. Ordering that Defendant engage third-party security auditors/penetration
28 testers as well as internal security personnel to conduct testing, including

- 1 simulated attacks, penetration tests, and audits on Defendant's systems on a
2 periodic basis, and ordering Defendant to promptly correct any problems or
3 issues detected by such third-party security auditors;
- 4 ii. Ordering that Defendant engage third-party security auditors and internal
5 personnel to run automated security monitoring;
- 6 iii. Ordering that Defendant audit, test, and train its security personnel regarding
7 any new or modified procedures;
- 8 iv. Ordering that Defendant segment employee data by, among other things,
9 creating firewalls and access controls so that if one area of Defendant's systems
10 is compromised, hackers cannot gain access to other portions of Defendant's
11 systems;
- 12 v. Ordering that Defendant purge, delete, and destroy, in a reasonably secure
13 manner, customer data not necessary for their provisions of services;
- 14 vi. Ordering that Defendant conduct regular database scanning and security
15 checks; and
- 16 vii. Ordering that Defendant routinely and continually conduct internal training
17 and education to inform internal security personnel how to identify and contain
18 a breach when it occurs and what to do in response to a breach.

19 **VII. PRAYER FOR RELIEF**

20 WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- 21 a. An order certifying this action as a class action under Federal Rule of Civil
22 Procedure 23, defining the Class as requested herein, appointing the
23 undersigned as Class counsel, and finding that Plaintiffs are proper
24 representatives of the Class requested herein;
- 25 b. A judgment in favor of Plaintiffs and the Class awarding them appropriate
26 monetary relief, including compensatory damages, punitive damages, attorney
27 fees, expenses, costs, and such other and further relief as is just and proper;
28

- 1 c. An order providing injunctive and other equitable relief as necessary to protect
2 the interests of the Class as requested herein;
- 3 d. An order requiring Defendant to pay the costs involved in notifying the Class
4 Members about the judgment and administering the claims process;
- 5 e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment
6 and post-judgment interest, reasonable attorneys' fees, costs, and expenses as
7 allowable by law; and
- 8 f. An award of such other and further relief as this Court may deem just and
9 proper.

10 **VIII. DEMAND FOR JURY TRIAL**

11 Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this First
12 Amended Class Action Complaint.

13 Dated: November 8, 2024

Respectfully submitted,

14
15 /s/: William B. Federman

William B. Federman

(admitted *pro hac vice*)

Kennedy M. Brian

(admitted *pro hac vice*)

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

T: (405) 235-1560

F: (405) 239-2112

E: wbf@federmanlaw.com

E: kpb@federmanlaw.com

22 **CERTIFICATE OF SERVICE**

23 I HEREBY CERTIFY that on November 8, 2024, I electronically filed the foregoing with
24 the Clerk of the Court using the CM/ECF system which will send notification of such filing to the
25 e-mail addresses denoted on the Electronic Mail notice list.

27 /s/: William B. Federman

28 William B. Federman

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 1

KEVIN MEAGHER

August 21, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear Kevin,

Kingdom Trust provides financial services to businesses, including The Loan Source, Inc. and ACAP SME, LLC, who provided services to you related to the U.S. Small Business Administration's Paycheck Protection Program, and has access to certain personal information as a result. The privacy and security of the personal information we maintain is of the utmost importance to Kingdom Trust. We are writing with important information regarding a recent data security incident that may have involved some of your personal information. We want to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On or around March 1, 2024, Kingdom Trust became aware of potential unauthorized access on our network.

What We Are Doing

Upon learning of this issue, we took steps to ensure the security of our systems and we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to assist us in determining the full extent of the incident and the scope of any data impacted and we also notified law enforcement. Based on the results of the investigation, we determined that certain data was subject to unauthorized access.

On or about August 1, 2024, after an extensive forensic investigation and manual document review, we discovered your personal information was included within the impacted data that may have been copied from our network as a result of the incident.

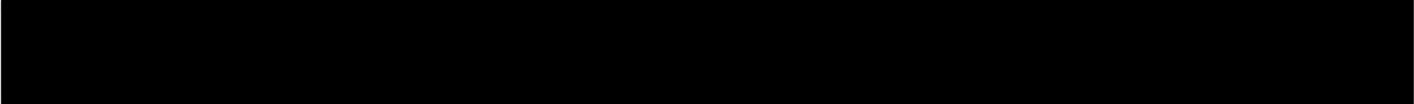
What Information Was Involved

The impacted files contained your full name and Social Security Number.

What You Can Do

We currently have no evidence indicating that any personal information has been used for identity theft or financial fraud as a result of the incident, however, out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.



In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.



For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated, confidential toll-free response line we have set up to respond to questions at 1-833-566-7612. The response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The response line is available between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Kingdom Trust
7336 W Post Road
Ste 111, Las Vegas, NV 89113



- OTHER IMPORTANT INFORMATION -**1. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	Experian P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289
--	--	---

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872
--	--	---

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164. **Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023. **New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <http://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226. **Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828. **New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/1/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. *In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal* As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

Rhode Island Residents: Under Rhode Island law, individuals have the right to obtain any policy report filed in regard to this event. You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400. There were approximately 3 Rhode Island residents that may be impacted by this incident.

EXHIBIT 2

WAO Fintech
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

REBECCA DAWSON

August 21, 2024

NOTICE OF DATA BREACH

Dear Rebecca,

Kingdom Trust provides financial services to businesses, including The Loan Source, Inc. and ACAP SME, LLC, who provided services to you related to the U.S. Small Business Administration's Paycheck Protection Program, and has access to certain personal information as a result. The privacy and security of the personal information we maintain is of the utmost importance to Kingdom Trust. We are writing with important information regarding a recent data security incident that may have involved some of your personal information as a Kingdom Trust client. We want to provide you with information about the incident and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On or around March 1, 2024, Kingdom Trust became aware of potential unauthorized access on our network.

What We Are Doing

Upon learning of this issue, we took steps to ensure the security of our systems and we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to assist us in determining the full extent of the incident and the scope of any data impacted and we also notified law enforcement. Based on the results of the investigation, we determined that certain data was subject to unauthorized access.

On or about August 1, 2024, after an extensive forensic investigation and manual document review, we discovered your personal information was included within the impacted data that may have been copied from our network as a result of the incident.

What Information Was Involved

The impacted files contained your full name and Date Of Birth, Email, Mobile.

What You Can Do

We currently have no evidence indicating that any personal information has been used for identity theft or financial fraud as a result of the incident, however, out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

In response to the incident, we are providing you with precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated, confidential toll-free response line we have set up to respond to questions at 1-833-556-7612. The response line is staffed with professionals familiar with this incident and knowledgeable about what you can do to protect against misuse of your information. The response line is available between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Kingdom Trust
7336 W Post Road
Ste 111, Las Vegas, NV 89113