

thousands of Defendant’s patients, including Plaintiff and the Class Members, had been exposed and obtained in a data breach. The information exposed and obtained by the attackers included Plaintiff’s and the Class Members’ demographic information, including names, dates of birth, addresses, phone numbers, and patient account numbers (collectively, “Personally Identifiable Information” or “PII”); clinical information, such as medical histories, diagnoses, and treatment plans with information relating to matters such as pregnancies, abortions, sexual partners, sexually transmitted diseases, genetic diseases, mental health diagnoses, and prescriptions (collectively, “Protected Health Information” or “PHI”); and health insurance information, including insurance plans, ID numbers, and claims information (*i.e.*, PHI).²

2. Ten months later, on January 30, 2024, Defendant sent an email to Plaintiff and the Class Members notifying them, for the first time, of the breach.

3. Defendant did not explain why it waited ten months to notify Plaintiff and the Class Members that Defendant’s systems had been breached and that Plaintiff’s and Class Members’ Private Information had been accessed ten months earlier and was in the possession of unknown third parties.

4. Plaintiff brings this class action against Defendant for its failure to

² This Complaint refers to PII and PHI collectively as “Private Information.”

secure and safeguard Plaintiff's' and Class Members' highly sensitive Private Information from unauthorized disclosure, exfiltration, and theft by third parties, and for its failure to timely and accurately notify Plaintiff and Class Members of the data breach.

5. Due to Defendant's inadequate data security, which breached duties imposed by law, unauthorized third parties gained access to Defendant's computer network and to highly valuable and highly sensitive PII and PHI belonging to Plaintiff and the Class Members.

6. Defendant is an OB/GYN physician service practice group that purports to be "one of the largest OB/GYN practices in the Southeast responsible for serving approximately 300,000 patients representing over 400,000 visits annually."³

7. In the course of providing OB/GYN care and treatment services to women across the Southeast, Defendant regularly acquired, collected, utilized, and derived a benefit from Plaintiff's and Class Members' PII and PHI. The PII at issue includes, but is not limited to, Plaintiff's and Class Members' names, addresses, dates of birth, phone numbers, and patient account numbers. The PHI at issue includes, but is not limited to, Plaintiff's and Class Members' medical

³ Atlanta Women's Health Group Website, <https://tinyurl.com/2rzksp5>, (last visited March 11, 2024).

histories, diagnoses, treatment plans, and health insurance information, including insurance plans, ID numbers, and claims information. Plaintiff's and Class Members' PII was stored in the same record set as Plaintiff's and Class Members' PHI, making the entire record set Protected Health Information.

8. As a condition of receiving OB/GYN care and treatment services, Defendant requires that its patients entrust them with PII and PHI.

9. As a healthcare provider that collects and stores patient PII and PHI, Defendant has statutory, regulatory, and common law duties to safeguard that information and ensure that it remains private, confidential, and protected against foreseeable criminal activity, and to timely and accurately notify patients of breaches compromising their PII and PHI. Defendant breached its statutory, regulatory, and common law duties as discussed herein.

10. A physician-patient relationship is a classic confidential and fiduciary relationship. "Confidential relations" are defined in Ga. Code Ann. § 23-2-58:

Any relationship shall be deemed confidential, whether arising from nature, created by law, or resulting from contracts, where one party is so situated as to exercise a controlling influence over the will, conduct, and interest of another or where, from a similar relationship of mutual confidence, the law requires the utmost good faith, such as the relationship between partners; principal and agent; guardian or conservator and minor or ward; personal representative or temporary administrator and heir, legatee, devisee, or beneficiary; trustee and beneficiary; and similar fiduciary relationships.

11. Defendant expressly and impliedly promised Plaintiffs and Class

Members that it would maintain the privacy and confidentiality of their PII and PHI. Defendant, as part of the medical services provided to Plaintiffs and Class Members, promised not to disclose their PHI without authorization. Plaintiffs and Class Members reasonably expected that their PII and PHI that they entrusted to Defendant, as part of their medical treatment, would remain confidential and would not be shared or disclosed to criminal third parties. The express and/or implied promises included an understanding that Defendant would take steps to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' PII and PHI. Defendant breached these duties by failing to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' PII and PHI.

12. On January 30, 2024, Defendant notified Plaintiff and Class Members via email of a “cyberattack” that its “security teams detected” on or around “April 12, 2023.” (hereafter, “Data Breach”). The email notice is attached as Exhibit 1.

13. Though the “cyberattack” was detected “on April 12, 2023,” upon information and belief the Defendant does not know when the attack occurred.

14. Defendant notified HHS of the Data Breach on June 11, 2023, within 60 days of April 12, 2023.

15. The January 30, 2024 email notice does not state why Defendant waited approximately ten months (from April 12, 2023 to January 30, 2024) to

notify Plaintiff and Class Members of the Data Breach.

16. After learning of the cyberattack in April 2023, Defendant claims to have launched a “robust” investigation led by “third-party forensic cybersecurity firms.” Exhibit 1.

17. According to the January 30, 2024 email notice, the Data Breach occurred when “unauthorized individuals gained access to our computer network and used ransomware to encrypt files.” Exhibit 1.

18. Defendant’s email notice confirms that an “unauthorized user accessed certain files containing personal information of a subset of AWHG patients.” Defendant’s forensic investigation concluded that “AWHGs electronic health record (EHR) systems remained secure and were not exposed in the breach,” but that “the files that were accessed held documents *containing protected health information* that may have included demographic information like names, dates of birth, addresses, phone numbers, and patient account numbers; *clinical information* such as medical history, diagnosis, and treatment plans; and *health insurance information*, including insurance plans, id numbers, and claims information.” Exhibit 1.

19. Upon information and belief, and based on the plain language of Defendant’s breach notice, Defendant improperly maintained PII and PHI, including “protected health information,” “clinical information,” and “health

insurance information” *outside of its EHR system*, in violation of statutory, regulatory, and common law duties and obligations.

20. In the January 30, 2024 email notice, AWHG says it “secured evidence that the unauthorized user permanently deleted all compromised data.” Exhibit 1. Thus, through the notice Defendant confirmed that the “unauthorized user” had in fact obtained and acquired PII and PHI in the first place. If the “unauthorized user” had not obtained and acquired the same data, then the “unauthorized user” would have had nothing to “delete.”

21. The January 30, 2024 email notice does not provide Plaintiff and other Class members with any proof that the “unauthorized user” in fact “permanently deleted all compromised data.” The notice does not explain why Defendant, or the Plaintiff and other Class members, should trust assurances about deletion of valuable, highly sensitive, PII and PHI from the same “unauthorized individuals” who successfully conducted a targeted cyberattack against one of the largest OB/GYN practices in the Southeast for the purpose of acquiring that valuable, highly sensitive, personal data.

22. Upon information and belief, Defendant AWHG does not know if the “unauthorized individuals” who carried out the cyberattack permanently deleted all compromised data *and* retained no copies.

23. Upon information and belief, the “unauthorized individuals” who

carried out the cyberattack are not honest brokers and were motivated to attack Defendant's system because of the valuable PII and PHI it holds from Plaintiff and the other Class members.

24. Upon information and belief, the "unauthorized individuals" who carried out the cyberattack were motivated to steal Plaintiff's and the other Class members' PII and PHI both because of the value of a ransom from Defendant and the value of data they stole from Defendant on the dark web and elsewhere.

25. The January 30, 2024 email notice claims that "not every patient was affected by this incident, but we are notifying all patients in an abundance of caution." Exhibit 1. Upon information and belief, Defendant does not know which of its patients' PII and PHI was compromised in the Data Breach because of Defendant's negligence in handling, maintaining, securing, encrypting, logging, and auditing the highly sensitive PII and PHI it requested and collected from Plaintiff and other Class members in the course of its business operations.

26. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address (1) Defendant's inadequate safeguarding of Plaintiff's and Class Members' PII and PHI that Defendant collected and maintained, and (2) Defendant's failure to provide timely and adequate notice to Plaintiff and other Class Members that their PII and PHI had been compromised in a cyberattack.

27. Plaintiff's and Class Members' PII and PHI was compromised due to

Defendant's negligent and/or careless acts and omissions and failure to protect the PII and PHI of Plaintiff and Class Members.

28. While many details of the Data Breach remain in the exclusive control of Defendant, upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable cyber threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents, and (10) failing to notify Plaintiff and Class Members in a timely and accurate manner so that they could mitigate the harm.

29. Defendant maintained Plaintiff's and the Class Members' PII and PHI in a negligent manner. In particular, the PII and PHI was maintained on computer

systems and networks that were in a condition vulnerable to cyberattack. The mechanism of the Data Breach, and the potential for improper disclosure of Plaintiff's and Class Members' PII and PHI, was a known risk to Defendant; and, thus, Defendant was on notice that failing to take appropriate protective measures would expose and increase the risk that the PII and PHI could be compromised and stolen.

30. As a result of Defendant's unreasonable and inadequate data security practices that resulted in the Data Breach, Plaintiff and Class Members have now been exposed to a present injury in the form of actual misuse of their PII and PHI and have further been exposed to an ongoing substantial, heightened, and imminent risk of financial fraud and identity theft for years to come. Plaintiff and Class Members must now and in the future closely monitor their financial accounts, credit reports, and tax returns to secure their accounts in an effort to deter and detect identity theft and fraud.

31. Because the exposed information included immutable personal details, Plaintiff and Class Members have suffered numerous actual and concrete injuries and damages that are personal, social, and financial, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft including purchasing credit monitoring services, credit freezes and other protective measures; (c) loss of time

and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their PII and PHI; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII and PHI, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ PII and PHI.

32. The PII and PHI of Plaintiff and Class Members are in the hands of hackers. Hackers routinely offer for sale the unencrypted, unredacted PII and PHI like that belonging to Plaintiff and Class Members that were compromised in the Data Breach. The exposed PII and PHI of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web. This risk will continue for Plaintiff’s and the Class Members’ respective lifetimes.

33. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII and PHI were accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendant’s data

security systems, and future annual audits.

34. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserts claims for: (i) breach of fiduciary duty, (ii) negligence, (iii) negligence *per se*, (iv) invasion of privacy/intrusion upon seclusion; (v) bailment; and, (vi) declaratory and injunctive relief.

PARTIES

35. Plaintiff M.T. is a Citizen of Georgia residing in Dekalb County, Georgia. Plaintiff received an email dated January 30, 2024, from Defendant AWHG notifying Plaintiff that Defendant's network had been breached and that Plaintiff's PII and PHI were compromised in the Data Breach.

36. Defendant Atlanta Women's Health Group, P.C. is a for profit domestic professional corporation organized under the laws of Georgia and headquartered in Atlanta, Georgia. Atlanta Women's Health Group, P.C.'s principal place of business is located at 5780 Peachtree Dunwoody Road, Suite 300, Atlanta, GA 30342. Defendant can be served through its registered agent, John Taylor, III, 5780 Peachtree Dunwoody Road, Suite 300, Atlanta, GA 30342.

37. Defendant is directly liable for its own acts, omissions, and negligence.⁴

⁴ Whenever reference is made in this Complaint to any action, inaction, or conduct of the Defendant named in this Complaint, the allegation is that the

JURISDICTION AND VENUE

38. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000, and there are more than 100 putative class members, and minimal diversity exists because, upon information and belief, Defendant and at least one Class Member are citizens of different States. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

39. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

40. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

Defendant engaged in the action, inaction, or conduct at issue by or through one or more of its officers, directors, agents, employees, or representatives who were engaged in the management, direction, control, or transaction of the ordinary business and affairs of the Defendant.

FACTUAL ALLEGATIONS

Defendant Promised to Protect Plaintiff's and Class Members' Highly Sensitive PII and PHI

41. Defendant is an OB/GYN physician practice group. Defendant's practices include Gynecology and Obstetrics. According to Defendant, "Atlanta Women's Health Group, P.C. is one of the largest OB/GYN practices in the southeast responsible for serving approximately 300,000 patients representing over 400,000 visits annually."

42. According to Defendant's website, examples of the services the Defendant's practices generally focus on within Gynecology and Obstetrics include abnormal bleeding, overactive bladder, surgical services (e.g., Hysterectomies, removal of ovaries and ovarian cysts, removal of uterine fibroids, removal of endometriosis, infertility evaluation, sterilization, abnormal Pap smear), pelvic pain, menopause, infertility, contraception, ultrasounds, family planning, vaginal revitalization, pediatrics/adolescents, and BioTE.

43. Based on patient intake forms used by Defendant, Defendant would keep the following highly sensitive personal health information in the ordinary course of maintaining a patient's medical history, diagnosis, and treatment plans: sexual history (e.g., number of sexual partners, sexual orientation), prior abortions, current medications, current health problems, surgeries, family health history, lab

work, mammograms, whether the person is menopausal, whether the person has had a hysterectomy, whether the person is pregnant, age of first menstrual period, date of last menstrual period, whether periods are regular, interval between periods, days of bleeding, heavy bleeding days, whether the person bleeds after intercourse, bleeding between periods, whether the person is in a sexual relationship (with male or female), whether the person has pain during sex, whether the person is trying to become pregnant, questions about sexual function, contraception or infections, type of contraception currently being used, types of contraception previously used, does the person use Depo-Provera, whether the person took a pregnancy test, problems with pregnancy (e.g., nausea, weight gain, weight loss, breast tenderness, pain, cramping, vomiting), Thalassemia, neural tube defect, congenital heart defect, Down Syndrome, Tay-Sachs, Canavan disease, Family Dysautonomia, Sickle cell disease or trait, Hemophilia or blood disorders, Muscular dystrophy, Cystic fibrosis, Huntington's chorea, Mental retardation, Autism, other inherited genetic chromosomal disorder, Maternal metabolic disorder, whether the patient or family members had a child with birth defects, recurrent pregnancy loss or stillbirth, and TB status.

44. In addition to the foregoing, Defendant maintains information regarding whether a patient or their partner have genital herpes, rash or viral illness, Hepatitis B or C, Chlamydia, Syphilis, HIV/AIDS, Gonorrhea, Genital

Warts, Public lice or crabs, Human Papilloma (HPV), and Trichomoniasis (Trich).

45. Defendant makes numerous commitments to its patients to protect their information. In its privacy policy, Defendant states at the very beginning that it is “committed to treating and using protected health information (“PHI”) about you responsibly.”⁵ Treating patient health information responsibly necessarily includes protecting it from a data breach.

46. Further, according to Defendant’s privacy policy, each time a patient visits the Defendant: “a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment.” This information, according to Defendant, may be used or disclosed to:

- Plan your care and treatment.
- Communicate with other providers who contribute to your care.
- Serve as a legal document.
- Receive payment from you, your plan, or your health insurer.
- Assess and continually work to improve the care we render and the outcomes we achieve.
- Comply with state and federal laws that require us to disclose your PHI.⁶

47. Defendant admits in its privacy policy that it has an obligation to maintain the privacy of a patient’s health information. And, if a breach occurs,

⁵ Privacy Policy and HIPAA, Atlanta Women’s Health Group, <https://awhg.org/privacy-policy-and-hipaa>, (last visited on Feb. 7, 2024).

⁶ *Id.*

Defendant states in its privacy policy that it will “[n]otify you in writing of a breach where your unsecured PHI has been accessed, acquired, used or disclosed to an unauthorized person.”⁷

48. Above all, the privacy policy promises that Defendant “will not use or disclose your PHI without your written authorization, except as described in this Notice.”⁸ Plaintiff and the Class Members did not authorize the Defendant to disclose their information to the threat actors behind the data breach.

49. Plaintiff and Class Members relied on Defendant’s representations that it would protect their personal and health information.

Plaintiff M.T.’s Experience

50. As a requisite to receiving medical services from Defendant, Plaintiff provided her PII and PHI to Defendant and trusted that the information would be safeguarded according to state and federal law. Upon receipt, PII and PHI was entered and stored on Defendant’s network and systems.

51. Plaintiff is very careful about sharing her sensitive PII and PHI. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

52. Plaintiff stores any documents containing her sensitive Private

⁷ *Id.*

⁸ *Id.*

Information in a safe and secure location or destroys the documents.

53. Had she known Defendant failed to follow basic industry security standards and failed to implement systems to protect her PII and PHI, she would not have provided that information to Defendant.

54. The notice email dated January 30, 2024 from Defendant notified Plaintiff that its network had been accessed and that Plaintiff's PII and PHI stored on its systems was involved in the Data Breach.

55. Furthermore, Defendant directed Plaintiff to be vigilant and to take certain steps to protect her Private Information and otherwise mitigate her damages.

56. As a result of the Data Breach, Plaintiff heeded Defendant's warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the email notifying her of the breach and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff to mitigate her damages by, among other things, monitoring her accounts for fraudulent activity.

57. Even with the best response, the harm caused to Plaintiff cannot be undone.

58. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII and PHI—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

59. She also lost her benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

60. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

61. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her PII and PHI being in the hands of unauthorized third parties and criminals.

62. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

63. Plaintiff has a continuing interest in ensuring that Plaintiff's PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

The Data Breach was Foreseeable and Defendant Should Have Foreseen the Risk of a Data Breach Involving Plaintiff's and the Class Members' PII and PHI

64. The injuries to Plaintiff and Class Members were reasonably

foreseeable to Defendant because common law, statutes, and industry standards required Defendant to safeguard its computer systems and employ reasonable procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the other Class Members' highly sensitive PII and PHI.

65. Defendant was obligated to perform its business operations in accordance with industry standards. Industry standards required Defendant to exercise reasonable care with respect to Plaintiff and the Class Members by implementing reasonable data security measures to mitigate foreseeable risk of harm to Plaintiff and the Class Members. Industry standards put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Defendant was the only entity responsible for adequately protecting Plaintiff's and the Class Members' data that Defendant alone solicited, collected, and stored.

66. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiff and Class Members and the risk of a data breach. Further, Defendant knew, or reasonably should have known, of the consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

67. In 2021, a record 1,862 data breaches occurred, resulting in

approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.⁹ The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

68. The healthcare industry continues to be a popular target for threat actors, which is why the United States Department of Health and Human Services (“HHS”) and other regulators have extensively focused on ensuring health care providers protect patient personal and health information. The last several years have seen multiple, high-profile health care breaches, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020).

69. Indeed, cyberattacks have become so common and notorious that the

⁹ See *2021 Data Breach Annual Report*, 6 (ITRC, Jan. 2022), <https://notified.idtheftcenter.org/s/> (attached as “Exhibit 2”).

FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁰

70. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹¹

71. Defendant knew or should have known that a data breach was reasonably foreseeable because the PII and PHI it stores for Plaintiff and Class Members is of high value to criminals. Indeed, the value of health information is considerably higher than the value of ordinary personal information, including credit cards. The FBI found that “[c]yber criminals are selling [health] information on the black market at a rate of \$50 for each partial [electronic health record], compared to \$1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription

¹⁰ FBI, *Secret Service Warn of Targeted*, Law360 (Nov.18,2019), <https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware> (attached as “Exhibit 3”).

¹¹ See Maria Hernandez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited April 2, 2024).

medication, and advance identity theft.”¹² *Forbes* reported in 2022 that the costs are now as high as \$1000 per health record.¹³

72. As detailed below, because of the variety of harms threat actors can inflict with both PII and PHI, PII and PHI are highly valuable to threat actors.

73. Given the frequency of cyberattacks in the healthcare industry, as well as the high value of PII and PHI, cybersecurity attacks were foreseeable to Defendant and should have been expected. The attendant risk of future attacks was widely known to Defendant.

Defendant’s Data Breach and Defendant’s Notice of Data Breach to Plaintiff and the Class Members

74. On January 30, 2024, Plaintiff received an email titled “AWHG Notice of Data Breach.”¹⁴ According to this email and a separate breach notification posting by Defendant on its website, Defendant identified “abnormal activity on its computer system” on April 12, 2023.¹⁵ Defendant claims that it then

¹² Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, 2 (Apr. 8, 2014), <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf> (last visited April 2, 2024).

¹³ Sanjay Cherian, *Healthcare Data: The Perfect Storm*, *Forbes* (Jan. 14, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/01/14/healthcare-data-the-perfect-storm/?sh=428f6a36c887> (last visited April 2, 2024).

¹⁴ Exhibit 1.

¹⁵ *Id.*; Atlanta Women’s Health Group, What Happened, https://awhg.org/multimedia/pdf/AWGH_Revised_Website_Document_2_6_2024.pdf (last visited on Feb. 8, 2024).

launched an investigation with the assistance of cybersecurity experts.

75. Defendant's Notice of Data Breach admits that Defendant's systems were accessed without authorization and that Plaintiff's and the Class Members' PII and PHI were compromised and taken by the threat actor.¹⁶

76. Defendant omits any information in its notice about when the attack may have first occurred, which is relevant to when the data may have first been put at risk.

77. According to Defendant, the threat actors (or, as Defendant blandly identifies them, the "unauthorized user") behind the attack were able to access files that held documents containing patients' names, dates of birth, addresses, phone numbers, account numbers, clinical information such as medical history, diagnosis and treatments plans, and health information including insurance plans, patient ID numbers, and claims information.

78. Neither the Plaintiff nor the Class Members whose information was accessed or taken by the threat actors authorized or consented to the threat actors accessing or acquiring their PII and PHI.

79. Upon information and belief, Plaintiff does now know which of its patients' PII and PHI was compromised in the Data Breach. That information is

¹⁶ *Id.*

in the exclusive province of the Defendant.

80. Defendant claims in its notice to Plaintiff that Defendant has “secured evidence that the unauthorized user permanently deleted all compromised data.” But this statement is at odds with the threat actors’ cyberattack, and it misleads Plaintiff and Class Members as to the risks to their data.

81. Class Members are left to reasonably conclude that their Private Information has been stolen by the threat actors and is still in their possession.

82. Defendant’s breach notification and letter raise additional questions about where Defendant stores patient data within its systems. Defendant acknowledges that patient health records were accessed by the threat actors and taken. Yet, Defendant’s notice to Plaintiff states that “AWHGs electronic health record (EHR) systems remained secure and were not exposed in the breach.” Defendant’s statement admits that patient information resided *outside* of the supposedly secure EHR systems, which violates HIPAA¹⁷ and industry standards, and is a grossly negligent data practice.

¹⁷ See 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, 164.316 & 164.530; see also Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, 42 U.S.C. § 1320d-2 (1996); U.S. Department of Health and Human Services, *Summary of the HIPAA Security Rule*, <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html> (last visited on February 6, 2024).

When Defendant Discovered the Breach vs. When It Told Patients About It

83. The HIPAA Breach Notification Rule has stringent requirements for health care providers to promptly notify affected patients: “A covered entity ***shall***, following the discovery of a breach of unsecured protected health information, ***notify each individual*** whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.”¹⁸ Such notice is to be provided “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.”¹⁹

84. In addition to requiring Defendant to notify affected patients, the HIPAA Breach Notification Rule also required Defendant to notify the Secretary of the United States Department of Health and Human Services (“HHS”) “following the discovery of a breach of unsecured protected health information[.]”²⁰

85. Here, because the breach involved more than 500 individuals, Defendant was required to notify HHS “contemporaneously with the notice

¹⁸ HIPAA Breach Notification Rule, 45 C.F.R. § 164.404(a)(1) (2013) (emphasis added).

¹⁹ HIPAA Breach Notification Rule, 45 C.F.R. § 164.404(b) (2013).

²⁰ HIPAA Breach Notification Rule, 45 C.F.R. § 164.408(a) (2013).

required by § 164.404(a) and in the manner specified on the HHS Web site.”²¹ In other words, Defendant was required to simultaneously notify *both* HHS *and* Plaintiff and the Class Members within 60 days of discovery of the breach.

86. Defendant claims it discovered the breach on April 12, 2023.

87. According to HHS, Defendant notified HHS on day 60—June 11, 2023.²²

88. Defendant did not notify Plaintiff and the Class Members on June 11, 2023. Indeed, Plaintiff and the Class Members were not notified of the Data Breach until January 30, 2024—nearly 10 months after Defendant discovered the breach. Defendant failed to promptly notify Plaintiff and the Class Members.

89. When Defendant finally did notify its patients about the Data Breach, it claimed that “in an abundance of caution” it was notifying all patients, including those who are not affected. If true, Defendant had even less reason to wait eight months after notifying HHS to notify its patients.

90. In addition to legal notification obligations arising under HIPAA, Defendant also had an ethical obligation to promptly notify its patients. According

²¹ HIPAA Breach Notification Rule, 45 C.F.R. § 164.408(b) (2013).

²² U.S. Department of Health and Human Services, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, (last visited on February 6, 2024).

to the American Medical Association (“AMA”):

When there is reason to believe that patients’ confidentiality has been compromised by a breach of the electronic medical record, physicians should:

(a) Ensure that patients are promptly informed about the breach and potential for harm, either by disclosing directly (when the physician has administrative responsibility for the EMR), participating in efforts by the practice or health care institution to disclose, or ensuring that the practice or institution takes appropriate action to disclose.”²³

91. Further, the AMA states that:

Physicians have a responsibility to follow ethically appropriate procedures for disclosure, which should at minimum include:

(c) Carrying out the disclosure confidentially and within a time frame that provides patients ample opportunity to take steps to minimize potential adverse consequences.

(d) Describing what information was breached; how the breach happened; what the consequences may be; what corrective actions have been taken by the physician, practice, or institution; and what steps patients themselves might take to minimize adverse consequences.²⁴

²³ AMA Code of Medical Ethics, Opinion 3.3.3 Breach of Security in Electronic Medical Records, American Medical Association, <https://code-medical-ethics.ama-assn.org/ethics-opinions/breach-security-electronic-medical-records#:~:text=When%20used%20with%20appropriate%20attention,%2C%20emotional%2C%20and%20dignitary%20harms>, (last visited on February 5, 2024)

²⁴ AMA Code of Medical Ethics, Opinion 3.3.3 Breach of Security in Electronic Medical Records, American Medical Association, <https://code-medical-ethics.ama-assn.org/ethics-opinions/breach-security-electronic-medical-records#:~:text=When%20used%20with%20appropriate%20attention,%2C%20emotional%2C%20and%20dignitary%20harms>, (last visited on February 5, 2024).

92. Defendant violated not just its legal obligations under the HIPAA Breach Notification Rule, but also its ethical obligations.

93. Further, Defendant violated its own privacy policy providing that it would timely and accurately notify patients of the compromise of their health information.

94. Defendant's late notification amplifies the harms, detailed in the sections below, that Defendant has caused Plaintiff and the Class Members through its negligent keeping of their PII and PHI.

95. By waiting to disclose the Data Breach and downplaying the risk that victims' PHI and PII would be misused by criminals, Defendant prevented victims from taking timely and proactive mitigation measures to protect themselves from harm.

96. Defendant's notification letter included "Recommended Steps to help Protect your Information" enclosure. Defendant did not offer identity theft protection but advertised the services of IDX so that patients could attempt to protect themselves from the harm Defendant's negligence caused them.

97. Unfortunately, as the GAO has observed in their research, "[c]onsumers have limited options to mitigate risks of other harms from data breaches, such as medical identity theft and identity theft tax refund fraud. Commercial identity theft services, credit freezes, and fraud alerts do not directly

address these risks.”²⁵

Defendant Violated HIPAA Security Rule Requirements

98. Defendant’s HIPAA violations extend beyond its untimely Data Breach notification. Health care providers subject to HIPAA, such as Defendant, are required to comply with and implement a number of security controls and safeguards to protect patient health information. Defendant did not do so.

99. Because PHI is so important, the first standard in the HIPAA Security Rule requires healthcare providers to safeguard it:

Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.²⁶

100. Given the frequency, likelihood, and cost of cyber- attacks, Defendant knew or should have known that a cyber-attack was foreseeable. Further, Defendant’s security controls and safeguards should have been designed

²⁵ United States Government Accountability Office, Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services, 13 (March 2019), <https://www.gao.gov/assets/gao-19-230.pdf> (last visited April 2, 2024).

²⁶ HIPAA Security Rule, 45 C.F.R. § 164.306(a) (2013).

to defend against exactly this type of attack.

101. Defendant should have deployed systems controls like encryption,²⁷ an “addressable” requirement set forth in the HIPAA Security Rule, and rendered patient health information unreadable to an attacker. Defendant did not do so.

102. The HIPAA Security Rule also requires covered entities to “[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).²⁸

103. Defendant’s email about the Data Breach states that the threat actors—who had not been “granted access rights”—nonetheless gained access to Plaintiff’s and the Class Members’ sacrosanct Private Information, evidencing Defendant’s failure to adequately implement this HIPAA requirement.

104. HIPAA requires other protections for access to health information. Covered entities must “[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”²⁹

²⁷ Defendant’s January 30, 2024 email notice did not disclose that the data obtained was encrypted; thus, the threat actors had access to unencrypted patient data. This is inexcusable given the extreme sensitivity of the data Defendant put at risk.

²⁸ HIPAA Security Rule, 45 C.F.R. § 164.312(a)(1) (2013).

²⁹ HIPAA Security Rule, 45 C.F.R. § 164.312(d) (2013).

105. The threat actors' ability to move around Defendant's system and access patient data demonstrates that Defendant also failed to satisfy this requirement.

106. The above are representative examples of Defendant's failure to meet its HIPAA Security Rule obligations.

Defendant Failed to Meet Basic Industry Standard Security Requirements

107. In addition to its multiple HIPAA Security Rule failings, Defendant also had a duty to implement reasonable security measures to protect the highly sensitive personal and health information of its patients. Defendant's duty correlates with the sensitivity of the data in Defendant's possession and control. In this case, Defendant's patients' data was perhaps the most sensitive data imaginable.

108. Further, Defendant is not a small one- or two-person clinic, but rather a large health group with ample resources to adequately protect its patients' data. Defendant's security obligations are far higher than the security Defendant implemented.

109. Numerous organizations, such as the FTC, the United States Cybersecurity and Infrastructure Security Agency ("CISA"), and the National Institute of Standards and Technology ("NIST") have defined the security controls and safeguards companies like Defendant must implement to protect consumer

information.

110. The FTC, for example, in its “Cybersecurity Basics” document, sets forth fundamental data security principles and practices. Among them: companies should encrypt devices and other media that contain sensitive personal information.³⁰ The FTC says such encryption should be used on “laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.”³¹ Further, the FTC states that companies should update their software, secure files, require passwords, use multi-factor authentication, secure routers, use WPA2 or WPA3 encryption, require strong passwords, train staff and generally have a plan for security.³² The FTC guidelines further recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.³³

111. Defendant could and should have implemented all of the above measures recommended by the FTC to prevent and detect cyberattacks. But, Defendant failed to implement one or more of the industry standard FTC

³⁰ FTC, *Cybersecurity Basics*, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics> (last visited on Feb. 26, 2024).

³¹ *Id.*

³² *Id.*

³³ [Protecting Personal Information: A Guide for Business | Federal Trade Commission \(ftc.gov\)](#) (last visited on March 4, 2024).

recommendations.

112. To prevent and detect ransomware attacks, like Defendant experienced, CISA in its #StopRansomware Guide recommends that companies like Defendant implement the following measures:

- Do not expose services, such as remote desktop protocol, on the web[.]
- Conduct regular vulnerability scanning to identify and address vulnerabilities[.]
- Regularly patch and update software and operating systems to the latest available versions[.]
- Ensure all on-premises, cloud services, mobile, and personal (i.e., bring your own device [BYOD]) devices are properly configured and security features are enabled[.]
- Limit the use of RDP and other remote desktop services[.]
- Implement phishing-resistant MFA for all services[.]
- Implement identity and access management (IAM) systems[.]
- Change default admin usernames and passwords[.]
- Do not use root access accounts for day-to-day operations[.]
- Store passwords in a secured database and use strong hashing algorithms[.]³⁴

113. Defendant could and should have implemented all of the above

³⁴ CISA, #StopRansomware Guide, <https://www.cisa.gov/stopransomware/ransomware-guide> (last visited on Feb. 26, 2024).

measures recommended by CISA to prevent and detect cyberattacks. But Defendant failed to implement one or more of the industry standard CISA recommendations.

114. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, the Microsoft Threat Protection Intelligence Team recommends 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

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface (“ASMI”)] for Office [Visual Basic for Applications (“VBA”)].³⁵

115. Because Defendant failed to properly protect and safeguard Plaintiff’s and Class Members’ PII and PHI by failing to implement one or more of the foregoing industry standard data security measures recommended by the FTC, CISA, and the Microsoft Threat Protection Intelligence Team, an unauthorized third party was able to access Defendant’s network and patient data.

Defendant Negligently Failed to Protect Plaintiff’s and Class Members’ PII and PHI in Violation of Defendant’s Duties and, Therefore, Caused the Data Breach

116. Defendant assumed and owed duties and obligations to Plaintiff and Class Members to take reasonable measures to maintain and protect the PII and

³⁵ [Human-operated ransomware attacks: A preventable disaster | Microsoft Security Blog](#) (last visited on March 4, 2024).

PHI that it regularly undertook to collect and store as part of its routine business operations.

117. Defendant breached its duties and obligations to Plaintiff and Class Members, and was negligent, because it failed to properly implement data security controls and safeguards that would adequately safeguard Plaintiff's and Class Members' PII and PHI. Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

- a. Failing to design and maintain adequate data security controls and safeguards to reduce the risk of data breaches and protect Plaintiff's and Class Members information;
- b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;
- c. Failing to test and assess the adequacy of its data security controls and safeguards;
- d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;
- e. Failing to implement uniform procedures and data security protections;
- f. Failing to maintain its patients' information solely in designated systems with the appropriate level of cybersecurity protections;
- g. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- h. Failing to ensure or otherwise require that it was compliant with HIPAA, FTC guidelines for cybersecurity, and other industry

standards and best practices;

- i. Failing to implement or update antivirus, endpoint detection and response software, and other intrusion detection and malware protection software;
- j. Failing to implement encryption or adequate encryption to protect its systems and patients' data, both while the data is at rest and while being transmitted; and
- k. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' information, which in turn allowed the threat actors to access and obtain such information.

118. Defendant failed to maintain reasonable and required security controls and safeguards for Plaintiff's and Class Members' PII and PHI.

119. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the information of Plaintiff and Class Members.

120. Defendant's negligence in safeguarding the information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

121. Despite the foreseeability of the Data Breach, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised, and those failures resulted in the Data Breach.

Background on the Harms that Victims of a Data Breach Suffer: Identity Theft and Financial Fraud, Medical Identity Theft, Out-of-Pocket Expenses, Lost Time, Worry, Stress, Humiliation, Shame, Loss of Trust in Healthcare System, and More

Identity Theft and Financial Fraud

122. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal personal and health information to monetize the information.

123. Criminals regularly monetize stolen data by selling it on the black market to other criminals who then commit a variety of identity theft related crimes, such as those discussed below. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

124. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information about a victim's identity, such as a person's login credentials or Social Security Number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as

spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

125. A sophisticated black market exists on the dark web where criminals can buy or sell personal and health information, like the information at issue in this case.³⁶ The digital character of personal information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity.³⁷ Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and health information.³⁸ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to

³⁶ The dark web is an unindexed layer of the internet that requires special software or authentication to access. What is the Dark Web? – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last visited April 2, 2024).

³⁷ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or ‘surface’ web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA’s web address is cia.gov, but on the dark web the CIA’s web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know. What Is the Dark Web?, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

³⁸ *Id.*; What Is the Dark Web?, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

others.”³⁹

126. According to the U.S. Government Accountability Office (“GAO”), regardless of how the data breach occurs, “[o]nce exposed, individuals’ information can be misused to commit identity theft, fraud, or inflict other types of harm.”⁴⁰

127. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.⁴¹ Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”⁴² Defendant did not rapidly report to Plaintiff and the Class Members that their information had been stolen.

128. Identity theft is not a speculative or unlikely occurrence. Indeed, the GAO noted that “[i]n 2016, according to the Bureau of Justice Statistics, an

³⁹ What is the Dark Web? – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

⁴⁰ United States Government Accountability Office, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services*, 4 (March 2019), <https://www.gao.gov/assets/gao-19-230.pdf>.

⁴¹ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> (last accessed October 21, 2022).

⁴² *Id.*

estimated 26 million people – 10 percent of U.S. residents aged 16 or older – reported that they had been victims of identity theft in the previous year.”⁴³

129. Victims of a data breach have a high degree of likelihood of being victims of identity theft. A January 2024 report by the U.S. Department of Justice Bureau of Justice Statistics reports “[v]ictims of identity theft [] were twice as likely as nonvictims [] to learn that an entity with their personal information experienced a data breach in the past year.”⁴⁴

130. The types of identity theft that may occur vary. The GAO described the following types of common identity theft:

- Financial fraud from identity theft, which can include
 - new-account fraud, in which thieves use identifying data, such as Social Security and driver’s license numbers, to open new financial accounts without that person’s knowledge; and,
 - existing-account fraud, which is more common and entails the use or takeover of existing accounts, such as credit or debit card accounts, to make unauthorized charges or withdraw money.
- Tax refund fraud, which occurs when a Social Security number or other personally identifiable information is used to file a fraudulent tax return seeking a refund.

⁴³ *Id.*

⁴⁴ U.S. Department of Justice Bureau of Justice Statistics, *Just the Stats: Data Breach Notifications and Identity Theft, 2021*, (January 2024), <https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021> (last visited April 2, 2024).

- Government benefits fraud, which occurs when thieves use stolen personal information to fraudulently obtain government benefits. For example, the Social Security Administration has reported that personal information of beneficiaries has been used to fraudulently redirect the beneficiary's direct deposit benefits.
- Medical identity theft, which occurs when someone uses an individual's name or personal identifying information to obtain medical services or prescription drugs fraudulently, including submitting fraudulent insurance claims.
- Synthetic identity theft, which involves the creation of a fictitious identity, typically by using a combination of real data and fabricated information. The federal government has identified synthetic identity theft as an emerging trend.
- Child identity theft, which occurs when a child's Social Security number or other identifying information is stolen and used to commit fraudulent activity.
- Other types of fraud that occur when personal information is used; for example, to set up mobile phone or utility accounts, or to engage in activities such as applying for employment or renting a home.⁴⁵

131. The U.S. Federal Trade Commission ("FTC") has also reported that:

"[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest."⁴⁶

⁴⁵ United States Government Accountability Office, Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services, 5-6 (March 2019), <https://www.gao.gov/assets/gao-19-230.pdf> (last visited April 2, 2024).

⁴⁶ Federal Trade Commission, Warning Signs of Identity Theft, <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last visited on Feb. 5, 2024).

132. Social Security numbers⁴⁷, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.

133. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing

⁴⁷ Defendant's data breach notice did not identify Social Security Numbers, but they are routinely collected and stored with the type of information accessed by the threat actor. Presently, information regarding the scope of the Data Breach is solely within the knowledge of Defendant. Plaintiff and Class Members do not presently know if their Social Security Numbers were accessed by the threat actor.

fraud activity to obtain a new number.⁴⁸

134. Even then, new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old [threat] information is quickly inherited into the new Social Security number.”⁴⁹ Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant being issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines.⁵⁰

⁴⁸ Social Security Administration, Identity Theft and Your Social Security Number, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited April 2, 2024).

⁴⁹ Brian Naylor, Victims of Social Security Number Theft Find It’s Hard to Bounce Back, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited April 2, 2024).

⁵⁰ Identity Theft and Your Social Security Number, Social Security Administration, 1 (2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited April 2, 2024).

Medical Identity Theft

135. The theft of health information is so uniquely harmful that the first standard in the HIPAA Security Rule requires health care providers to secure protected health information.

136. While health information can be used by threat actors for the types of identity theft described above by GAO, “medical identity theft” raises special risks.

137. In a World Privacy Forum report, medical identity theft was described as follows:

Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity — such as insurance information — without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name.⁵¹

138. The FTC has a similar definition: “Medical identity theft is when someone uses your personal information — like your name, Social Security number, health insurance account number or Medicare number — to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance

⁵¹ Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum, 6 (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf (last visited April 2, 2024).

provider, or get other medical care.”⁵² “If the thief’s health information is mixed with yours, it could affect the medical care you’re able to get or the health insurance benefits you’re able to use. It could also hurt your credit.”⁵³

139. Victims of medical identity theft experience several harms, such as:

- “Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can then affect the healthcare a person receives if the errors are not caught and corrected.”
- “Significant bills for medical goods and services they neither sought nor received.”
- “Issues with insurance, co-pays, and insurance caps.”
- “Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.”
- “Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime, in the aftermath of the crime.”
- “Data gathered in the last 5 years and data analyzed for this report sheds new facts and light on the seriousness of debt collection problems for victims. Victims can experience long term problems with aggressive medical debt collection arising from debt that does not belong to them. As a result of improper or even potentially fraudulent medical debt reporting, some victims may not qualify for mortgage or other loans and may experience other financial impacts.”
- “Phantom medical debt collection based on medical billing or other identity information is an additional modality of harm.”

⁵² Federal Trade Commission, *What to Know About Medical Identity Theft*, <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Feb. 5, 2024).

⁵³ *Id.*

- “Sales of medical debt arising from identity theft can perpetuate a victim’s debt collection and credit problems, through no fault of their own.”
- “Victims still experience a general lack of ability to cure the full range of problems medical identity theft brings, even over the course of years for some victims.”⁵⁴

140. Complicating these harms is the fact that “[m]edical forms of identity theft are difficult to fix after the fact” and complications from identity theft can last for years.⁵⁵

141. The harm from medical identity theft is enduring. The World Privacy Forum report observed that “[medical identity theft] can cause significant and often enduring harms to its victims, and it has left a trail of victims who have suffered deeply.”⁵⁶ Indeed, the harms “develop over sometimes long periods of time. The consequences of medical identity theft still remain among the most severe of all identity crimes, and time has not lessened the severity of consequences victims may experience.”⁵⁷

⁵⁴ Pam Dixon and John Emerson, The Geography of Medical Identity Theft, World Privacy Forum, 6-7 (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf (last visited April 2, 2024).

⁵⁵ *Id.*

⁵⁶ Pam Dixon and John Emerson, The Geography of Medical Identity Theft, World Privacy Forum, 6 (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf (last visited April 2, 2024).

⁵⁷ *Id.*

Out-of-Pocket Expenses, Lost Time, Worry, Stress, Humiliation, Shame, Loss of Trust in Healthcare System, and More

142. Victims of a breach of their personal health information not only face harms like identity theft, medical identity theft, and financial fraud, but also out-of-pocket expenses, lost time, worry, stress, humiliation, shame, loss of trust in the healthcare system and providers, and more.

143. The President’s Identity Theft Task Force released a report stating that in addition to the potentially thousands of dollars in out-of-pocket expenses incurred by victims of a data breach, victims “have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves.”⁵⁸

144. Indeed, victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

145. Because data thieves may wait years before attempting to use stolen

⁵⁸ The President’s Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, 11 (April 2007), <https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf> (“Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.”) (last visited April 2, 2024).

data, Plaintiff and Class Members will need to remain vigilant for years to come.

146. Where the personal health information compromised in a data breach concerns highly sensitive medical history, treatment, and diagnostic materials—like it does here—the embarrassment, humiliation, worry, and risk of blackmail increases.⁵⁹ The AMA has found that “when a security breach occurs, patients may face physical, emotional, and dignitary harms.”⁶⁰

147. Further, data breaches erode trust patients have in their doctors. If a patient must worry that their doctor will have a data breach and their sensitive health information may be publicly exposed, the patient may hold back on sharing vital health information with their doctor. In response to this concern, AMA’s “Privacy Principles” state: “[a]bove all, patients must feel confident that their health information will remain private. Preserving patient trust is critical.”⁶¹

⁵⁹ See, e.g., Charles Ornstein, Small-Scale Violations of Medical Privacy Often Cause the Most Harm, ProPublica, (Dec. 10, 2015), <https://www.propublica.org/article/small-scale-violations-of-medical-privacy-often-cause-the-most-harm> (last visited April 2, 2024).

⁶⁰ AMA Code of Medical Ethics, Opinion 3.3.3 Breach of Security in Electronic Medical Records, American Medical Association, <https://code-medical-ethics.ama-assn.org/ethics-opinions/breach-security-electronic-medical-records#:~:text=When%20used%20with%20appropriate%20attention,%2C%20emotional%2C%20and%20dignitary%20harms>, (Last visited on Feb. 5, 2024).

⁶¹ See Robert J. Mills, *AMA Issues New Principles to Restore Trust in Data Privacy*, Press Release Point (May 11, 2020), <https://www.pressreleasepoint.com/ama-issues-new-principles-restore-trust-data-privacy>; American Medical Association, *AMA Privacy Principles*, (May 2020),

COMMON INJURIES & DAMAGES

148. As result of Defendant's inadequate data security, Plaintiff and Class Members now face significant harms, including identity theft, medical identity theft, fraud, out-of-pocket expenses, lost time, worry, stress, humiliation, shame, loss of trust in the healthcare system, and more.

149. Due to the foreseeable Data Breach, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution of value of their personal and health information; and (i) the continued risk to their personal and health information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect

<https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf> (last visited April 2, 2024).

Plaintiff's and Class Members' information.

150. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, a reasonable person is expected to take steps and spend time learning about the breach and mitigating the risks of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater harm—yet, the resource and asset of time is lost.

151. The Defendant's email regarding the Data Breach says that Plaintiff and Class Members should “remain vigilant by reviewing your account statements and credit reports closely.”

152. Likewise, the FTC recommends that data breach victims take certain steps after a breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁶²

153. Because of the Data Breach, Plaintiff and Class Members have spent

⁶² See Federal Trade Commission, Identity Theft.gov, <https://www.identitytheft.gov/Steps> (last visited April 2, 2024).

and will spend time in the future on a variety of prudent actions, such as reviewing and monitoring credit reports and accounts for unauthorized activity, placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, and filing police reports.

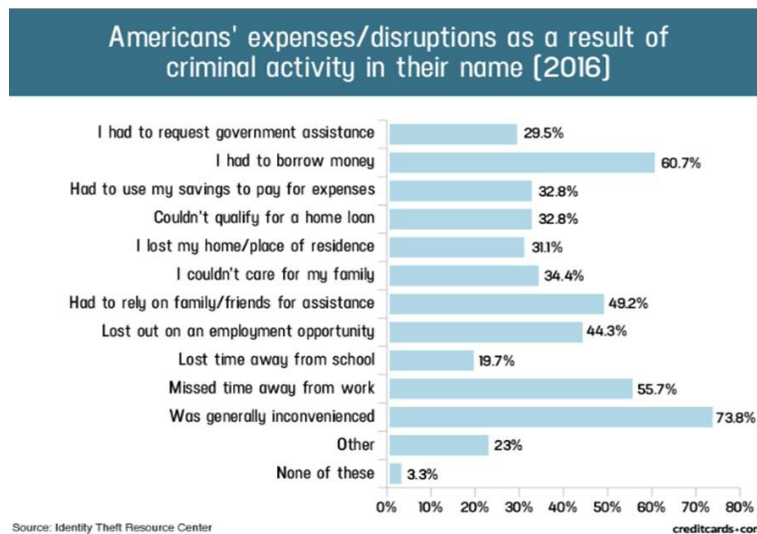
154. Plaintiff and Class Members bear a significant and costly burden to mitigate the harms they face due to Defendant’s negligence in handling and securing their Private Information.

155. Even with Plaintiff and Class Members making their best efforts to mitigate the harms from Defendant’s negligence, Plaintiff and Class Members are still at significant risk of identity theft because of the Data Breach.

156. In the event that Plaintiff and Class Members experience actual identity theft and fraud, a 2007 GAO Report regarding data breaches states that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

157. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information after a data

breach:⁶³



158. Separate and apart from harms related to identity theft and fraud, as a result of the Data Breach the monetary value of Plaintiff's and Class Members' Private Information has been diminished by its unauthorized acquisition by threat actors and release onto the dark web (where it may soon be available and holds significant value for the threat actors).⁶⁴ As with any product or commodity, the value of data is directly tied to its scarcity and usefulness. Because of the Data

⁶³ "Credit Card and ID Theft Statistics" by Jason Steele, 06/11/2021, at <https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/> (last visited March 28, 2024).

⁶⁴ Private Information, like that at issue here, is currency. Companies trade and sell Private Information, like that at issue here. Marketing firms use Private Information to target potential customers, and an economy exists related to the value of Private Information. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

Breach, Plaintiff's and Class Members' PII and PHI is now more readily available (potentially on the dark web) and is less valuable.

Future Cost of Credit and Identify Theft Monitoring Is Reasonable and Necessary

159. To date, Defendant has *not* provided Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach.

160. The Private Information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information or bank information which cost between \$10 and \$25.⁶⁵ The Private Information accessed and disseminated in this case included “[c]omplete medical records [which] can be particularly valuable to identity thieves, and may go for up to \$1,000.”⁶⁶ The Private Information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

161. Consequently, Plaintiff and Class Members are at a present and

⁶⁵ See Jesse Damiani, Your Social Security Number Costs \$4 On The Dark Web, New Report Finds, FORBES (Mar.25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1> (last visited April 2, 2024).

⁶⁶ What Is the Dark Web?, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited April 2, 2024).

ongoing risk of fraud and identity theft for many years into the future.

162. Given the targeted attack here, the sacrosanct, highly-sensitive Private Information stolen, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, and will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims’ names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

163. There may be a substantial time lag—years or longer—between when harm occurs and when it is discovered, and when Private Information is stolen and when it is used. According to GAO, which conducted a study regarding data breaches: “[S]tolen 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.”⁶⁷

164. Such fraud may go undetected until debt collection calls commence

⁶⁷ Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed April 2, 2024).

months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

165. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Injunctive Relief Is Necessary to Protect Against Future Data Breaches

166. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to be in the possession of Defendant, is protected from further breaches by Defendant's implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

167. Plaintiff brings this nationwide class action on behalf of herself and on

behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

168. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendant in January 2024, including all who were sent a notice of the Data Breach on or around January 30, 2024 (the “Class”).

169. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

170. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

171. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are in excess of 33,000 individuals whose PII and PHI may have been improperly

accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

172. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiff and Class Members;
- b. Whether Defendant had duties not to disclose the PII and PHI of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the PII and PHI of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PHI and PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Defendant violated the consumer protection statutes invoked herein;
- l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

173. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII and PHI compromised as a result of the Data Breach, due to Defendant's misfeasance.

174. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies

hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

175. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

176. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could

afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

177. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

178. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, uniform methods of data collection, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

179. Adequate notice can be given to Class Members directly using

information maintained in Defendant's records.

180. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Petition.

181. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

182. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant made promises to Plaintiff and Class Members,

through Defendant's privacy policy or otherwise, regarding handling of Plaintiffs' and Class Members' Private Information, and the terms of those promises;

- e. Whether Defendant breached promises made in its privacy policy or otherwise to Plaintiff and Class Members;
- f. Whether Defendant timely, adequately, and accurately informed Plaintiff and Class Members that their PII and PHI had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the of Plaintiff and Class Members; and
- i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I: BREACH OF FIDUCIARY DUTY

183. Plaintiff and the Class Members re-allege and incorporate by reference the allegations of paragraphs 1-182 of this Complaint as if they were fully restated herein.

184. At all relevant times, the physicians and other healthcare providers providing medical care and treatment to patients at Defendant AWHG were employees and/or agents of Defendant AWHG and were acting in the course and

scope of said capacity.

185. As a result of the patient- doctor relationship, Defendant has a fiduciary relationship with Plaintiff and Class Members.

186. Because of the special doctor-patient relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (a) for the safeguarding of Plaintiff's and Class Members' Private Information; (b) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (c) to maintain complete and accurate records of what information (and where) Defendant stored that information.

187. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with its patients, in particular, to keep secure their Private Information.

188. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' Private Information.

189. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their Private Information to unauthorized third parties.

190. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including

but not limited to: (a) invasion of privacy; (b) financial “out of pocket” costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued imminent and continuing risk to their Private Information, which remains in Defendant’s possession, and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information.

191. As a direct and proximate result of Defendant’s breach of its fiduciary duty, Plaintiff and Class Members are entitled to compensatory, consequential, and general damages suffered as a result of the Data Breach, or in the alternative, nominal damages.

192. Plaintiff and the Class Members also seek punitive damages against Defendant for Defendant’s breaches of the fiduciary duties arising from the confidential relationship between physicians and their patients.

193. As shown above, Defendant breached its confidential relationship

with Plaintiff and the other Class Members by the reckless manner in which Defendant exposed the Plaintiff's and the Class Members' PII and PHI to exploitation by hackers. As such, Defendant is liable for compensatory damages.

194. After Defendant knew of the breach, Defendant *intentionally* exposed Plaintiff and the Class Members to *greater harm* by failing to disclose to Plaintiff and the Class Members for approximately ten months that hackers had gained access to Plaintiff's and the Class Members' PII and PHI, and thus, Defendant intentionally violated their duties arising from this confidential relationship.

195. Defendant's willful and intentional decision not to disclose the data breach to its patients deprived Plaintiff and the Class Members of the opportunity to take proactive steps to mitigate the harm of the disclosure of the PII and PHI for months and months.

196. As such, Defendant's actions evidenced willful misconduct, malice, fraud, wantonness, and that entire want of care which would raise the presumption of conscious indifference to consequences, thus making Defendant liable for punitive damages.

197. When Defendant intentionally elected not to disclose the breach to Plaintiff and the Class Members, and thus decided to expose Plaintiff's and the Class Members' most sensitive health information to repeated and continuing

exploitation over many additional months, Defendant acted with specific intent to cause harm, which subjects Defendant to punitive damages with no “cap.”

COUNT II:
NEGLIGENCE

198. Plaintiff and the Class repeat paragraphs 1 – 182 of the Complaint as if fully set forth herein.

199. Plaintiff and Class Members were required to submit their PII and PHI to Defendant in order to receive healthcare services from Defendant.

200. In providing their PII and PHI, Plaintiff and Class Members had a reasonable expectation that this information would be securely maintained and not easily accessible to, or exfiltrated by, cybercriminals. That reasonable expectation was informed, at least in part, by Defendant’s privacy policy.

201. Upon receiving the PII and PHI of Plaintiff and Members of the Class in the ordinary course of its healthcare services business, Defendant owed to Plaintiff and the Class Members a duty of reasonable care in handling, maintaining, storing, and using the same PII and PHI, in securing and protecting the information from being stolen, accessed, and misused by unauthorized parties, and in notifying Plaintiff and Class Members promptly and accurately in the event of a data breach.

202. Defendant’s duty of care was imposed by law, assumed by behavior, and/or voluntarily undertaken by Defendant. First, Defendant’s duty of care arose

as a result of the special fiduciary relationship that existed between Defendant and its patients. Second, Defendant's duty of care arose under HIPAA, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. 164.530(c)(1). Third, Defendant's duty of care arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. Fourth, Defendant's duty of care arose under industry standards providing that companies, like Defendant, must use reasonable care in securing and protecting confidential PII and PHI that it either acquires, maintains, or stores from foreseeable risks, including cyberattacks. Fifth, Defendant's duty of care arose under its privacy policy, in which it promised to exercise care in safeguarding PII and PHI and to notify affected patients if data was compromised. Sixth, Defendant's duty of care arose due to the known high frequency of cyberattacks in the healthcare space, and the fact that the harm to patient victims in a healthcare data breach (here, the Plaintiff and Class Members) exceeds the costs to Defendant of taking reasonable steps to mitigate the risks of a data breach.

203. Defendant owed a duty of care to Plaintiff and the Class Members

because Plaintiff and the other Class members compose a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant requested and collected PII and PHI from their patients (including Plaintiff and the other Class Members) for the purpose of providing healthcare services to its patients, and the patients (including Plaintiff and the other Class Members) entrusted their PII and PHI to Defendant for the purpose of obtaining healthcare services from Defendant.

204. Because of these duties, Defendant was required to, among other things, take reasonable steps in accordance with industry standards to: safeguard and prevent disclosure of PII and PHI; design, maintain, and test its data security systems to ensure that these systems were reasonably secure and capable of protecting the PII and PHI of Plaintiff and the Class Members in the event of a foreseeable data breach; implement systems and procedures that would detect a breach of their security systems in a timely manner and to timely act upon security alerts from such systems; notify affected patients promptly and accurately in the event of a data breach; train its data security professionals to ensure their knowledge and competence in safeguarding and protecting highly sensitive PII and PHI.

205. Attendant to Defendant's duties, and Defendant's collection, use, and

storage of Plaintiff's and Class Members' PII and PHI, Defendant knew or should have known of its inadequate and unreasonable security practices with regard to their systems and also knew that hackers and thieves routinely attempt to access, steal, and misuse the types of PII and PHI that Defendant requested and collected from its patients who entrusted Defendant with their data. As such, Defendant knew a breach of its systems would cause damage to its patients and Plaintiff and the other Class members. Thus, Defendant had a duty to act reasonably in protecting the PII and PHI of its healthcare clients' patients.

206. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII and PHI, as alleged and discussed herein, including by:

- a. Acting unreasonably in collecting, storing, and maintaining the Private Information and failing to exercise reasonable care in its implementation of its security systems, protocols, and practices in order to sufficiently protect the PII and PHI of Plaintiff and Class Members;
- b. Negligently designing and maintaining its data security system in a manner that failed to secure Plaintiff's and Class Members' PII and PHI from unauthorized access;
- c. Implementing inadequate security controls;
- d. Implementing inadequate security products;

- e. Implementing inadequate security policies, including with respect to password protection policies and use of multi-factor authentication for its systems;
- f. Failing to properly monitor its data security systems for data security vulnerabilities and risk;
- g. Failing to test and assess the adequacy of its data security system;
- h. Failing to develop and put into place uniform procedures and data security protections for its healthcare network;
- i. Allocating insufficient funds and resources to the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;
- j. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;
- k. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;
- l. Designing its systems without encryption or without adequate encryption;
- m. Failing to comply with its own Privacy Policy;
- n. Failing to comply with regulations protecting the PII and PHI at issue during the period of the Data Breach;
- o. Maintaining Plaintiff's and Class Members' PII and PHI outside its EHR

system;

p. Failing to recognize in a timely manner that PII and PHI had been compromised;

q. Waiting for over nine months before it disclosed the Data Breach; and

r. otherwise negligently and affirmatively mishandling Plaintiff's and Class Members' PII and PHI provided to Defendant, which in turn allowed cybercriminals to access its computer network.

207. Defendant had a duty to promptly and accurately notify Plaintiff and the Class Members of the Data Breach so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct alleged herein.

208. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members face current and ongoing foreseeable risks, including identity theft, and compensatory damages sustained by Plaintiff and Class Members including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and

imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendant’s possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ Private Information.

209. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

210. Defendant’s negligent conduct is ongoing, in that it still holds the PII and PHI of Plaintiff and Class Members in an unsafe and unsecure manner.

211. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT III:
NEGLIGENCE *PER SE*

212. Plaintiff and the Class repeat and re-allege paragraphs 1 - 182 of the

Complaint as if fully set forth herein.

213. Under 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

214. Under HIPAA, Defendant had a duty to act reasonably in collecting, storing, and maintaining the PII and PHI, and to use reasonable security measures. HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. 164.530(c)(1). HIPAA's implementing regulations, HIPAA's Security Rule, and the HHS publications described above also form part of the basis of Defendant's duty in this regard.

215. Defendant violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the

foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class Members from a data breach due to the valuable and sensitive nature of the PII and PHI at issue in this case.

216. Defendant's violations of Section 5 of the FTC Act and HIPAA constitute negligence *per se*.

217. Plaintiff and Class Member are within the class of persons that the FTC Act and HIPAA were intended to protect.

218. The harm that occurred because of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of the failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiff and Members of the Class.

219. Plaintiff and Class Members are entitled to compensatory, consequential, and general damages. Plaintiff and Class Members are also entitled to nominal damages suffered as a result of the Data Breach.

220. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated and "impacted" individuals whose PII and PHI was accessed during the Data Breach, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of

identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial “out of pocket” costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) anxiety, annoyance and nuisance, (i) nominal damages, and (j) the future costs of identity theft monitoring.

221. Moreover, Plaintiff’s and Class Members’ PII and PHI remain at risk, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff’s and Class Members’ PII and PHI.

222. Therefore, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity theft monitoring to all Class Members.

COUNT IV:
INVASION OF PRIVACY /
INTRUSION UPON SECLUSION

223. Plaintiff and the Class repeat and re-allege paragraphs 1–182 of the Complaint as if fully set forth herein.

224. The State of Georgia recognizes the tort of Intrusion into Seclusion,

and has adopted the Restatement (Second) of Torts, which states:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

225. Defendant required that Plaintiff and Class Members provide PII and PHI to Defendant in order to receive services from Defendant, and Plaintiff and Class Members wanted and expected their PII and PHI to remain private and non-public.

226. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in the PII and PHI Defendant collected and stored.

227. Defendant's intentional conduct of collecting, storing, and using Plaintiff's and Class Members' PII and PHI is akin to surveillance of their PII and PHI, which is Private Information.

228. Defendant actively participated in the intrusion into Plaintiff's and Class Members' affairs by negligently maintaining Plaintiff's and Class Members' PII and PHI, by choosing deficient data security measures despite the known risks of a catastrophic data breach, by failing to protect Plaintiff's and Class Members' Private Information and allowing unauthorized and unknown third parties to access the Private Information of Plaintiff and Class Members, and by failing to

promptly and accurately notify Plaintiff and Class Members so that they could take steps to mitigate the harm caused by the Data Breach.

229. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and Class Members is highly offensive to a reasonable person.

230. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by intentionally misusing and disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

231. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members entrusted their Private Information to Defendant as a prerequisite to their use of Defendant's services, but they did so privately with the intention that their Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that their Private Information would be kept private and would not be disclosed without their authorization due to Defendant's privacy policy, among other reasons.

232. Defendant's inadequate data security practices and the resulting Data Breach constitute intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private

affairs or concerns, of a kind that would be highly offensive to a reasonable person.

233. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it knew or should have known that its data security practices were inadequate and insufficient.

234. Because Defendant acted with this knowing state of mind, it had notice and knew its inadequate and insufficient data security practices would cause injury and harm to Plaintiff and Class Members.

235. By intentionally failing to keep Plaintiff's and Class Members' Private Information secure, and by intentionally misusing and disclosing Private Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy and right to seclusion by, *inter alia*: a. Intentionally and substantially intruding into their private affairs in a manner that would be highly offensive to a reasonable person; b. Intentionally publicizing private facts about Plaintiff and Class Members, which is highly offensive and objectionable to an ordinary person; c. Intentionally invading their privacy by improperly using their Private Information properly obtained for another purpose, or disclosing it to unauthorized persons; and d. Intentionally causing anguish or suffering to Plaintiff and Class Members.

236. The Private Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included PII and PHI that is

the type of sensitive Private Information that one normally expects will be protected from exposure by the entity charged with safeguarding it. Defendant's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

237. Defendant's unlawful invasions of privacy damaged Plaintiff and Class Members. As a direct and proximate result of Defendant's unlawful invasions of privacy, Plaintiff and Class Members suffered mental distress, and their reasonable expectations of privacy were frustrated and defeated.

238. As a direct and proximate result of Defendant's public disclosure of private facts, Plaintiff and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains

in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

239. Plaintiff and Class Members are entitled to compensatory, consequential, general and nominal damages suffered as a result of the Data Breach.

240. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT V:
BAILMENT

241. Plaintiff and the Class repeat and re-allege paragraphs 1 – 182 of the Complaint as if fully set forth herein.

242. Plaintiff's and Class Members' PII and PHI is personal property.

243. Plaintiff and Class Members delivered and entrusted their PII and PHI to Defendant for the purpose of receiving healthcare services from its healthcare providers.

244. Plaintiff and Class Members provided their PII and PHI to Defendant

on the express and implied conditions that it had a duty to keep the PII and PHI confidential.

245. In delivering their PII and PHI to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard their PII and PHI.

246. Defendant therefore acquired and was obligated to safeguard the PII and PHI Plaintiff and Class Members.

247. Plaintiff's and Class Members' PII and PHI have commercial value and are highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the PII and PHI for safeguarding and assumed the risk voluntarily.

248. Once Defendant accepted Plaintiff's and Class Members' PII and PHI, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once it was within the possession, custody, and control of Defendant.

249. Defendant accepted possession and took control of Plaintiff's and Class Members' Private Information under such circumstances that the law imposes an obligation to safeguard the property of another. Accordingly, a bailment was established for the mutual benefit of the parties.

250. Specifically, a constructive bailment arises when a defendant, as is

the case here, takes lawful possession of the property of another and has a duty to account for that property, without intending to appropriate it.

251. Constructive bailments do not require an express assumption of duties and may arise from the bare fact of the thing coming into the actual possession and control of a person fortuitously, or by mistake as to the duty or ability of the recipient to effect the purpose contemplated by the absolute owner.

252. During the bailment, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their PII and PHI.

253. Defendant did not safeguard Plaintiff's or Class Members' PII and PHI when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

254. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class Members' PII and PHI, resulting in the unlawful and unauthorized access to and misuse of such Private Information.

255. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages.

COUNT VI:
DECLARATORY AND INJUNCTIVE RELIEF

256. Plaintiff and the Class repeat and re-allege paragraphs 1 – 182 of the Complaint as if fully set forth herein.

257. Plaintiff and Class Members pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

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

259. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' PII and PHI, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their PII and PHI. Plaintiff and the Class remain at imminent risk that further compromises of their PII and PHI will occur in the future.

260. The Court should also issue prospective injunctive relief requiring

Defendant to employ adequate security practices consistent with law and industry standards to protect Plaintiff's and Class Members' PII and PHI.

261. Defendant still possesses the PII and PHI of Plaintiff and the Class.

262. To Plaintiff's knowledge, Defendant has made no announcement that it has changed its data storage or security practices relating to the PII and PHI.

263. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

264. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial.

265. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendant's obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their PII and PHI and Defendant's failure to address the security failings that led to such exposure.

266. There is no reason to believe that Defendant's employee training and security measures are any more adequate now than they were before the breach to meet Defendant's obligations and legal duties.

267. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at Defendant, Plaintiff and Class Members will likely continue to be subjected to fraud, identity theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

268. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and Class.

269. Plaintiff and Class Members therefore, seek a declaration (1) that Defendant's existing data security measures do not comply with its obligations and duties of care to provide adequate data security, and (2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage internal security personnel to conduct testing, including audits on Defendant's systems, on a periodic basis, and ordering Defendant to promptly correct any

- problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
 - c. Ordering that Defendant audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;
 - d. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;
 - e. Ordering that Defendant conduct regular database scanning and security checks; and
 - f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Class, and appointing Plaintiff and her

Counsel to represent the Class;

- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII and PHI of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the

privacy interests of Plaintiff and Class Members;

- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiff and Class Members;
- v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- viii. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

- ix. requiring Defendant to conduct regular database scanning and securing checks;
- x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
- xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiii. requiring Defendant to implement, maintain, regularly review, and

revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

- E. For an award of punitive as allowed by law in an amount to be determined by an enlightened jury;
- F. For an award of attorneys' fees, costs, and litigation expenses under O.C.G.A. Section 13-6-11 and as otherwise allowed by law;
- G. For prejudgment interest on all amounts awarded; and
- H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 3, 2024

Respectfully Submitted,

/s/ MaryBeth V. Gibson

MaryBeth V. Gibson
GA Bar No. 725843
Gibson Consumer Law Group, LLC
4729 Roswell Road
Suite 208-108
Atlanta, GA 30342
Telephone: (678) 642-2503
marybeth@gibsonconsumerlawgroup.com

/s/ David H. Bouchard

Michael Sullivan
Ga. Bar No. 691431
David H. Bouchard
Ga. Bar No. 712859
Gabriel Knisely
Ga. Bar No. 367407
Finch McCranie, LLP
229 Peachtree St., NE, Suite 2500
Atlanta, GA 30303
(404) 658-9070
msullivan@finchmccranie.com
david@finchmccranie.com
gabe@finchmccranie.com

/s/ Todd McClelland

Todd McClelland
GA Bar No. 483301
Sterlington, PLLC

One World Trade Center
285 Fulton St., 85th Floor
New York, NY 10007
todd.mcclelland@sterlingtonlaw.com
(212) 433-2993

Counsel for Plaintiff and Putative Class

LOCAL RULE 7.1 CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing pleading filed with the Clerk of Court has been prepared in 14-point Times New Roman font in accordance with Local Rule 5.1(C).

Date: April 3, 2024.

/s/ David H. Bouchard
David H. Bouchard
GA Bar No. 712859

Exhibit 1

From: Comprehensive Women's OB GYN Dwdy <no-reply@eclinicalmail.com>
Date: January 31, 2024 at 9:11:53 AM EST
To: [Redacted]
Subject: AWHG Notice of Data Breach



January 30, 2024

Notice of Data Breach

Dear [Redacted],

We respect the privacy of your information and value the trust you place in us, which is why we are writing to let you know about a data security incident affecting Atlanta Women's Health Group (AWHG).

What Happened

AWHG has confirmed that unauthorized individuals gained access to our computer network and used ransomware to encrypt files. AWHG security teams detected the cyberattack on April 12, 2023, and steps were immediately taken to contain the attack. Third-party forensic cybersecurity firms were engaged immediately to investigate the potential breach.

The forensic investigation was robust and ultimately determined that while the unauthorized user accessed certain files containing personal information of a subset of AWHG patients, AWHG's electronic health record (EHR) systems remained secure and were not exposed in the breach. There is no evidence that any of the accessed information has been improperly used and AWHG has secured evidence that the unauthorized user permanently deleted all compromised data. We feel strongly that any information obtained was not used for malicious intent. Nevertheless, we are notifying every patient of this event. To be clear, not every patient was affected by this incident, but we are notifying all patients in an abundance of caution.

What Information Was Involved

AWHG and our third-party forensic cybersecurity firm has conducted a thorough review and determined that the files that were accessed held documents containing protected health information that may have included demographic information like names, dates of birth, addresses, phone numbers, and patient account numbers; clinical information such as medical history, diagnosis, and treatment plans; and health insurance information, including insurance plans, id numbers, and claims information. Again, after extensive investigation, we do NOT believe any of our patients information has been misused, but we are notifying you in an abundance of caution.

What We Are Doing

AWHG values your privacy, and we deeply regret that this incident occurred. Since this event, AWHG has worked with our outside security consultant to implement additional cybersecurity measures to prevent recurrence of such an attack and to protect the privacy of our valued patients, including replacing certain components of our system and upgrading security measures.

What You Can Do

Again, at this time, there is no evidence that your information has been misused. However, we

encourage you to remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

For More Information

Should you need further information and assistance, please use the toll-free number 1-888-566-8248, Monday through Friday between 9 a.m. - 9 p.m. Eastern Time. Additional recommended steps to help protect your information is also included with this letter.

Sincerely,



Genevieve Fairbrother MD, MPH, MHHCM, FACOG
President and CEO Atlanta Womens Health Group
(Enclosure)



Recommended Steps to help Protect your Information

1. Telephone. Contact IDX at 1-888-566-8248 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to https://link.edgepilot.com/s/22cf56ba/HKHW810g6U6S5zt8ZtZ3_Q?u=http://www.annualcreditreport.com/ or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly. You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experians or Equifax website. A fraud alert

tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-888-298-0045 P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000
https://link.edgepilot.com/s/0ef2fa74/_sVZi7Nq-Uezd3FvkgAf1w?u=http://www.equifax.com/personal/credit-report-services/	https://link.edgepilot.com/s/962eb552/5Ggdg2DpxU2NEcuZlwYU6Q?u=http://www.experian.com//help	https://link.edgepilot.com/s/49ce2ad0/ID0zcCf26kGOjj0IKD_c0A?u=http://www.transunion.com//credit-help

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (<https://link.edgepilot.com/s/a27d6772/wbR7rZ0nkEWSQvb-7YHLAW?u=http://www.oag.ca.gov/privacy>) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, https://link.edgepilot.com/s/876d095e/_jPX8CaSj0WgVl2c4NcFIQ?u=http://www.ag.ky.gov/, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division

200 St. Paul Place Baltimore, MD 21202,

<https://link.edgepilot.com/s/25c54613/NdlBzwYf10CnOqsRNO8djQ?u=http://www.oag.state.md.us/Consumer>, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit prescreened offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting

https://link.edgepilot.com/s/aeae1426/7Kp4ZJsHt0Cy9lvatnQHRw?u=http://www.consumerfinance.gov/f/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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755;

<https://link.edgepilot.com/s/43c68db3/ppxp0NJmo06Qrub3pnHQzw?u=https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001,

https://link.edgepilot.com/s/186ea427/CMz6oBb4qE_w7xUR2rRATA?u=http://www.ncdoj.gov/, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, <https://link.edgepilot.com/s/b50e255a/s1VAYt3likWMOL59PFJVA?u=http://www.doj.state.or.us/>, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903,

<https://link.edgepilot.com/s/dce8668a/bfpzAsZl006dx4VzvYQa7Q?u=http://www.riag.ri.gov/>,

Telephone: 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. At this time, there are no known Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580,

https://link.edgepilot.com/s/4269bda0/O9aNAT6DbUifW_gIPogzPg?u=https://consumer.ftc.gov/, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

If you wish to opt out from receiving these notifications in the future, you can [Unsubscribe](#).

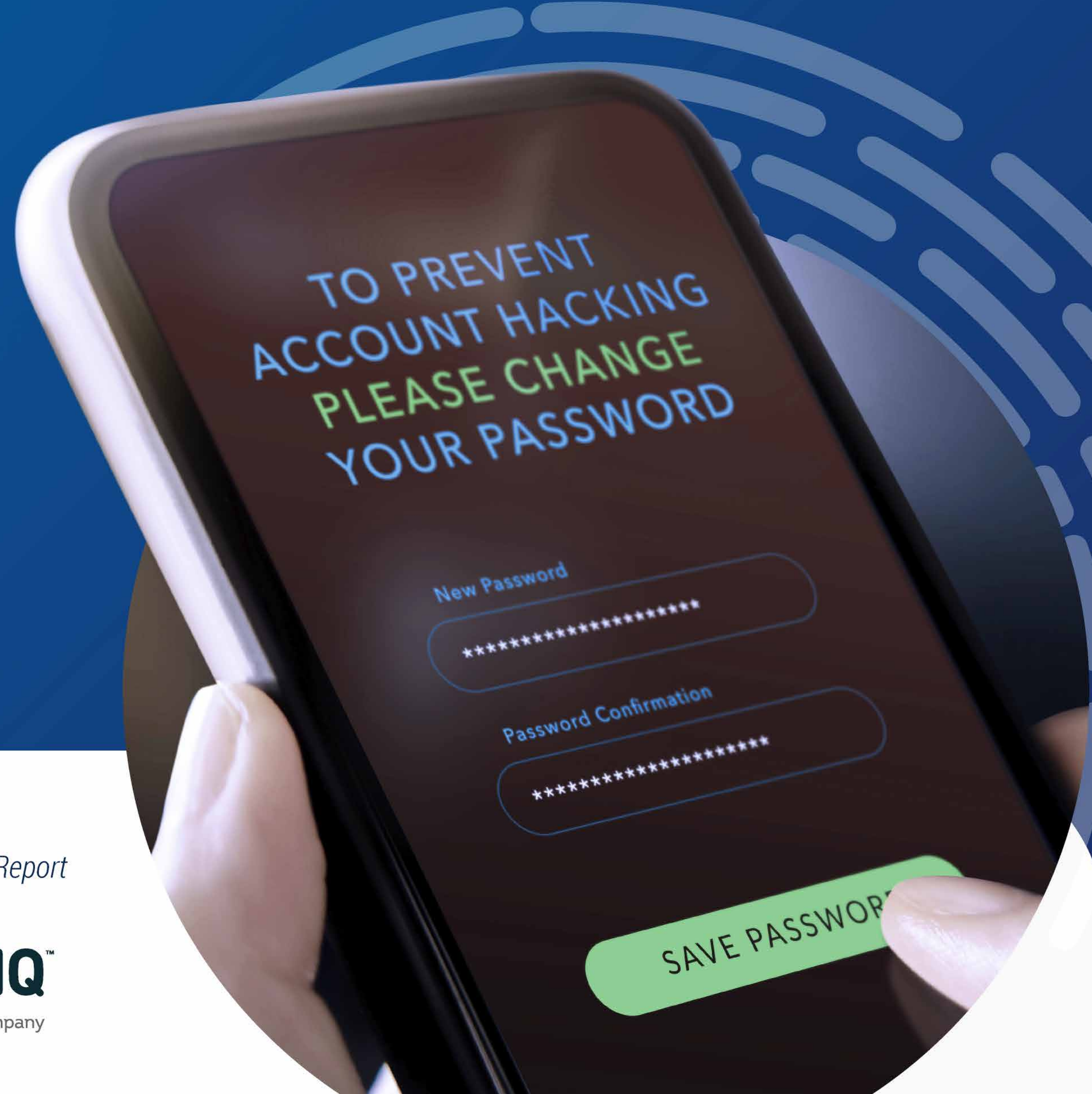
Exhibit 2

2021 in review

Data Breach

ANNUAL REPORT

Identity Compromises: From the Era of Identity Theft to the Age of Identity Fraud



IDENTITY THEFT
RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

The 2021 Data Breach Report
is supported by:



Table of Contents

I. Letter from the CEO	3	VII. Case Studies	18
II. Executive Summary	5	A. Accellion – Supply Chain Attack	
A. Compromise Trends 2015 to 2021		B. Robinhood - Social Engineering	
III. Number of Compromises in 2021	7	C. T-Mobile - Vulnerable Security	
IV. Root Cause of Compromises	8	VIII. ITRC Breach Alert Services (<i>notified</i> TM)	22
A. Cyberattacks		IX. Appendix	24
B. Human & System Errors		A. Data Breaches/Exposures Q4	
C. Physical Attacks		B. Data Breaches/Exposures Q3	
V. Types of Data Compromised	11	C. Data Breaches/Exposures Q2	
A. Exposed Data/ Breaches 2017 through 2021		D. Data Breaches/Exposures Q1	
B. Compromises Involving Sensitive Records		X. Glossary of Terms	28
C. 2021 Breached Data Attributes		XI. Data Sources & Methodology	29
D. Supply Chain Attack Data 2017 through 2021			
VI. Notable Trends	15		

Letter from the CEO



Eva C. Velasquez

(President & CEO, ITRC)

January 2022

In 2021, there were **more data compromises reported** in the United States of America **than in any year** since the first state data breach notice law became effective in 2003.

There are a number of watershed moments in the history of cybercrime. The first cyberattack was in 1834 when criminals intercepted bond trading information sent by a mechanical telegraph system in

France. The modern era of cyberattacks began in 1957 when a blind, seven-year-old child discovered they could whistle a tone that would allow them to make long-distance telephone calls for free.

We may very well look back at 2021 as the milestone year when we officially moved from the era of identity theft to an era of identity fraud. That is to say, the time when cybercriminals shifted from mass data accumulation (identity theft) to mass data misuse (identity fraud). Fueling most identity fraud-related crimes was consumer information stolen from businesses in data breaches.

Individuals were often caught in the crossfire between professional cybergangs and organizations that hold consumer information in trust. The personal information of consumers remained valuable to cybercriminals, but individuals were not the primary target for most identity crimes committed in 2021. Instead, consumer information was often the means to the end of attacking businesses through stolen credentials – logins and pass-

words – or social engineering where savvy cybercriminals tricked people into revealing information needed to launch an attack.

To be sure, consumers are still at risk and there are still cybercriminals looking to separate trusting people from their resources. But the vast majority of data compromises that occur today represent highly sophisticated, highly complex cyberattacks that require aggressive defenses to prevent. If those defenses fail, we too often see a level of transparency that is inadequate for consumers to protect themselves from identity fraud.

To help ensure more consumers learn when their personal information is at risk due to a data compromise, we are launching a new, free data breach alert service later in Q1 2022. We hope giving consumers more timely information and more relevant advice will help reverse a trend we recently identified in new research:

Less than 5 percent take the most effective protective action after receiving a data breach notice.

In our modern, digital-driven world, it is impossible to separate data, privacy, and identity protection. Yet, our current **legal, regulatory, and policy**

frameworks at the state and federal levels of government do not adequately address the growing and evolving threats that data breaches represent to individuals, organizations, and society as a whole.

It is not the ITRC’s purpose or place to name and shame organizations that have experienced a data compromise, but we do advocate for solutions to these issues. It is also our mission to inform public policy makers of the risks and benefits of addressing or ignoring the rise in identity crimes. It is also our job to point out that the needs of identity crime victims are at risk of being lost in the discussions of how to reduce cyber threats. And, it is our duty to share our knowledge so that individuals, organizations, and institutions can make informed decisions about how to protect themselves and those in their care from the criminals who would misuse our personal information.

This report reflects our mission and the current state of identity risks. In the pages that follow, the data will speak for itself. I hope that you will find it both informative and motivational to help us find more ways to prevent identity crimes and support identity crime victims.

Finally, please join me in thanking **Sontiq**, a TransUnion Company, for their support of this Report. Without the generous support of partners like Sontiq and our other **public, private, and government partners**, we would not be able to provide the research and analysis of important trends, identity education programs, or identity crime victim assistance.

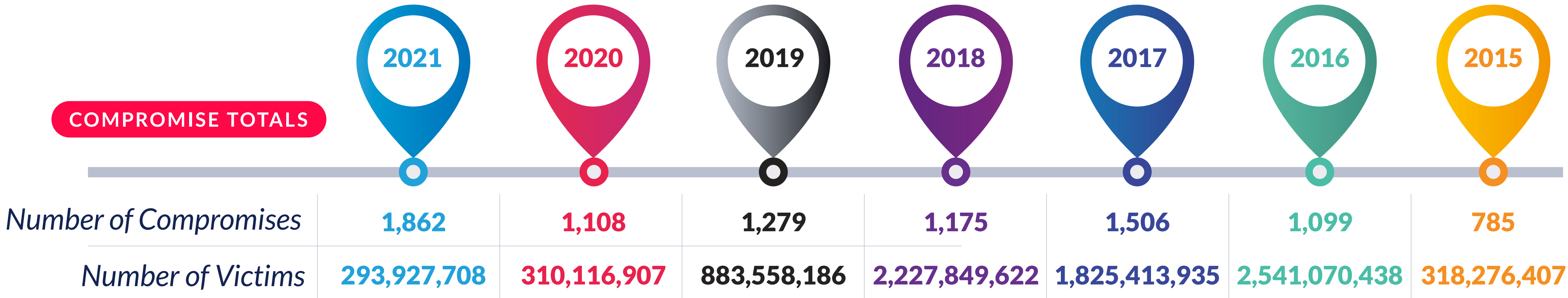
Executive Summary

The overall number of data compromises (1,862) is up **68 percent** over 2020; the new record number of data compromises is **23 percent** over the previous all-time high (1,506).

- + The number of data events that involved sensitive information such as SSNs increased slightly YoY as a percent of the overall number of compromises (83 percent vs. 80 percent), but remained well below the previous all-time high of 95 percent set in 2017.
- + Ransomware-related data breaches have doubled in each of the past two years. At the current growth rate, ransomware attacks will pass Phishing as the number one root cause of data compromises in 2022.

- + The number of data breach notices that do not reveal the root cause of a compromise (607) has grown by more than 190 percent since 2020.
- + The number of supply chain attacks, where a single organization is attacked to obtain the data of multiple entities, is obscured by the root cause these compromises (e.g. phishing, ransomware, malware, etc.). In 2021, supply chain attacks would be classified as the fourth most common attack vector if a stand-alone cause.
- + There were more cyberattack-related data compromises (1,613) in 2021 than all data compromises in 2020 (1,108).
- + Compromises increased year-over-year in every primary sector but one - Military where there were no data breaches publicly disclosed. The Manufacturing & Utilities sector saw the largest percentage increase in data compromises at 217 percent over 2020.
- + As identity criminals focus more on specific data types rather than mass data acquisition, the number of victims continues to drift downward - ~5% in 2021 compared to the previous year. The number of consumers whose data is compromised multiple times per year, though, remains excessively high.

Compromise Trends 2015 to 2021



ATTACK VECTOR TRENDS

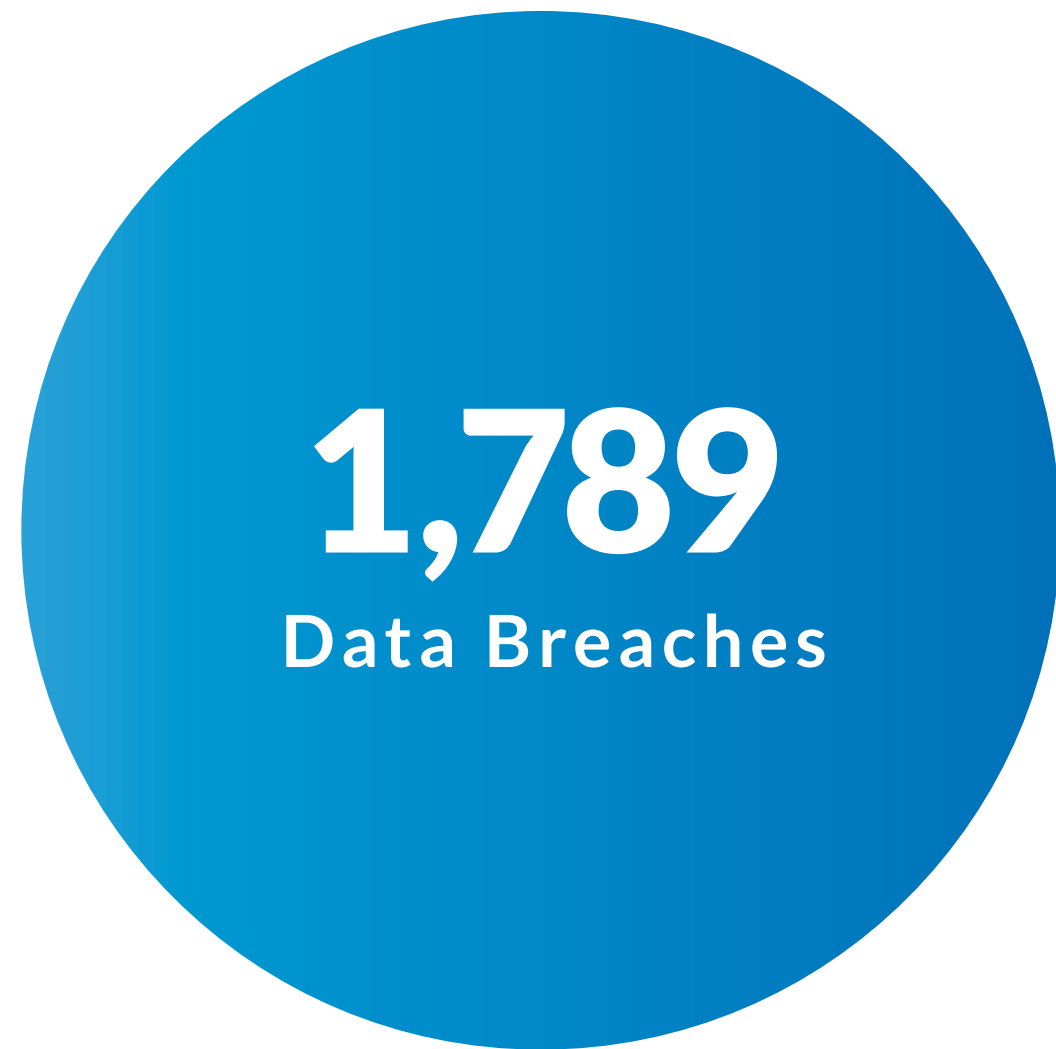
	2021	2020	2019
Cyberattacks	1,613	878	928
Phishing/Smishing/BEC	537	383	490
Ransomware	321	158	83
Malware	139	104	112
Non-secured Cloud Environment	23	51	15
Credential Stuffing	14	17	3
Unpatched software flaw	4	3	3
Zero Day Attack	4	1	n/a
Other - not specified	436	161	222
NA	106	n/a	n/a
Human & System Errors	179	152	231
Failure to configure cloud security	54	57	56
Correspondence (email/letter)	66	55	89
Misconfigured firewall	13	4	4
Lost device or document	12	5	19
Other - not specified	34	31	63
Physical Attacks	51	78	118
Document Theft	9	15	19
Device Theft	17	30	57
Improper Disposal	5	11	14
Skimming Device	1	5	4
Other - not specified	19	17	24
Unknown	12	n/a	2

SECTOR TRENDS

	2021		2020		2019	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	125	1,680,300	42	978,254	71	5,161,005
Financial Services	279	19,745,846	138	2,687,084	172	103,939,736
Government	66	3,244,455	47	1,100,526	64	1,193,791
Healthcare	330	28,045,658	306	9,700,238	398	9,080,498
Hospitality	33	217,941	17	22,365,384	40	1,459,393
Manufacturing & Utilities	222	49,775,124	70	2,896,627	103	70,265,156
Military	--	--	--	--	1	1,243
Non-Profit/NGO	86	2,309,008	31	37,528	36	248,824
Professional Services	184	22,697,765	144	73,012,132	84	1,694,188
Retail	102	7,186,143	53	10,710,681	86	370,128,202
Technology	79	44,035,156	67	142,028,859	62	107,923,851
Transportation	44	534,280	21	1,208,292	15	211,335
Other	308	79,223,368	172	43,391,302	147	212,250,964
Unknown	4	35,232,664	--	--	--	--

Number of Compromises in 2021

 **1,862** compromises
 **293,927,708** victims



 **189,532,878** victims



 **104,392,275** victims
 **6,993,145,763**
total records exposed



 **1,823,449,287** victims*
 **11,659,060,239**
total records exposed

*Includes non-U.S victims

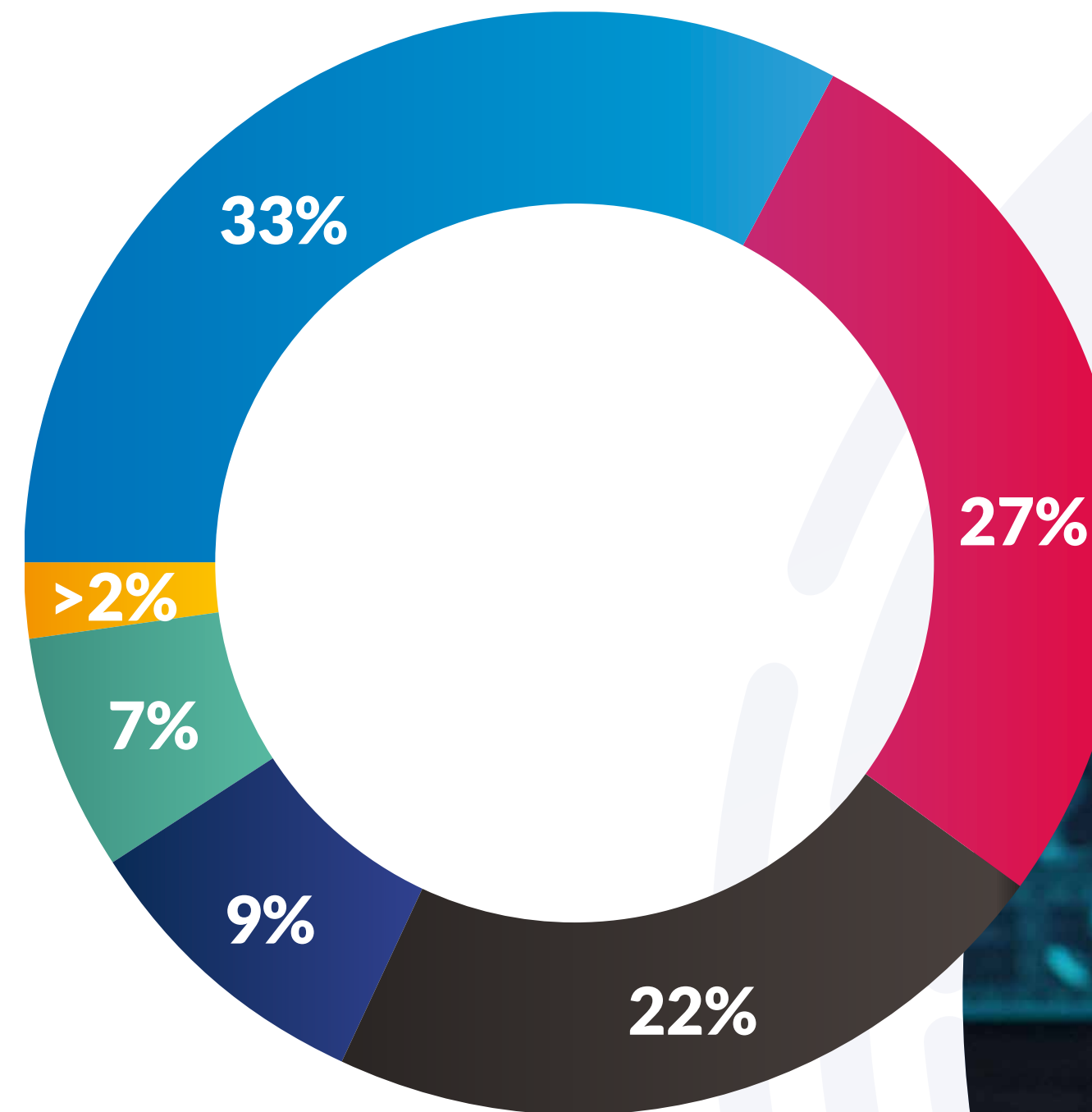


 **2,555** individuals impacted

Root Cause of Compromises

Cyberattacks

Cause	Qty	%
Phishing/Smishing/BEC	537	33%
Ransomware	350	22%
Malware	139	9%
Non-secured Cloud Environment	23	1%
Credential Stuffing	14	1%
Unpatched software flaw (CVE)	4	0.2%
Zero Day Attack	4	0.2%
Other - not specified	436	27%
NA	106	7%

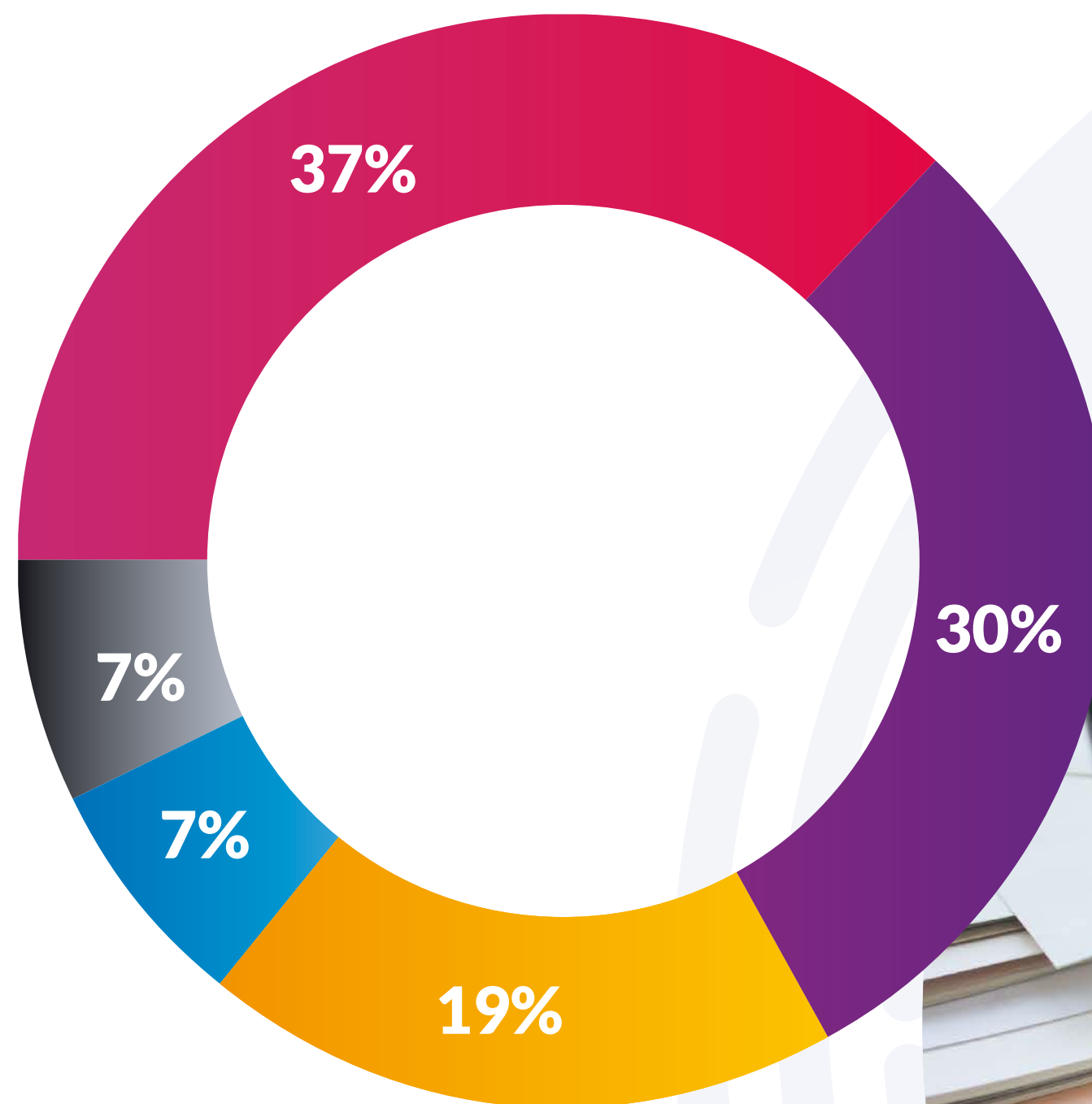


 **1,613** breaches/exposures
 **188,900,415** victims

Human & System Errors

Cause / Qty / %

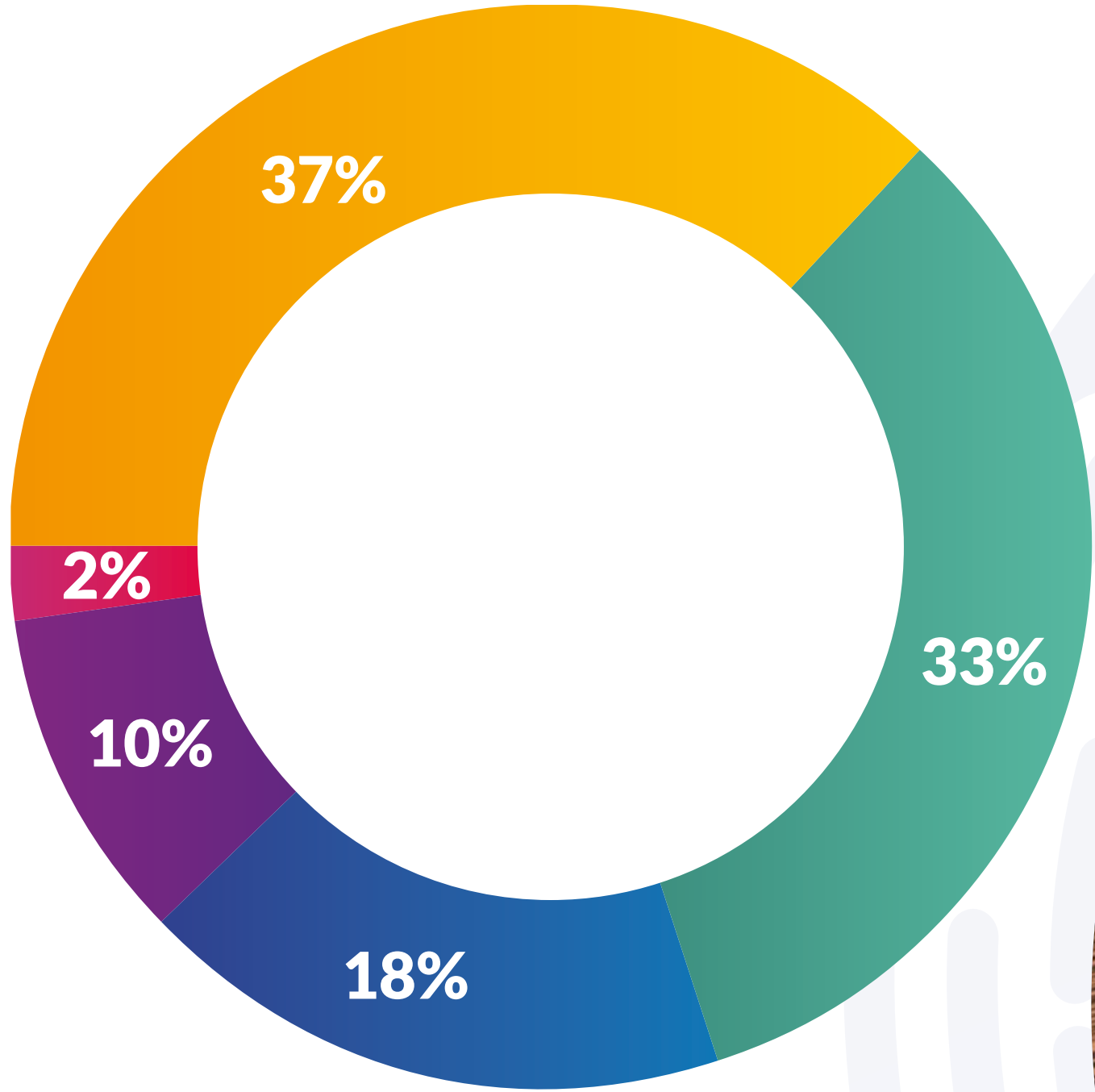
Correspondence (email/letter)	66	37%	●
Failure to configure cloud security	54	30%	●
Misconfigured firewall	13	7%	●
Lost device or document	12	7%	●
Other - not specified	34	19%	●



 **179** breaches/exposures
 **104,891,759** victims

Physical Attacks

Cause	Qty	%
Device Theft	17	33%
Document Theft	9	18%
Improper Disposal	5	10%
Skimming Device	1	2%
Other - not specified	19	37%



51 breaches/exposures



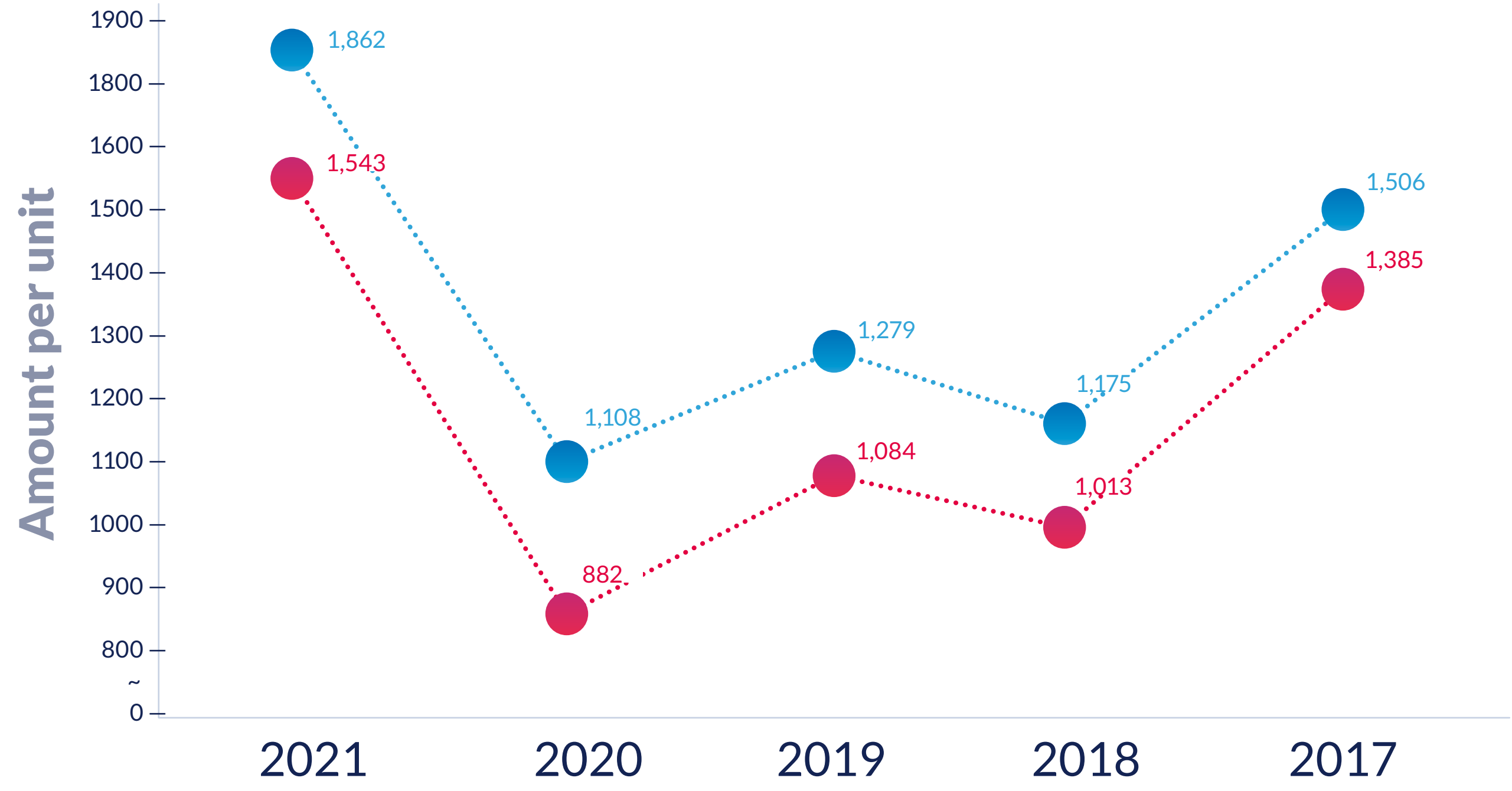
132,979 victims

Types of Data Compromised

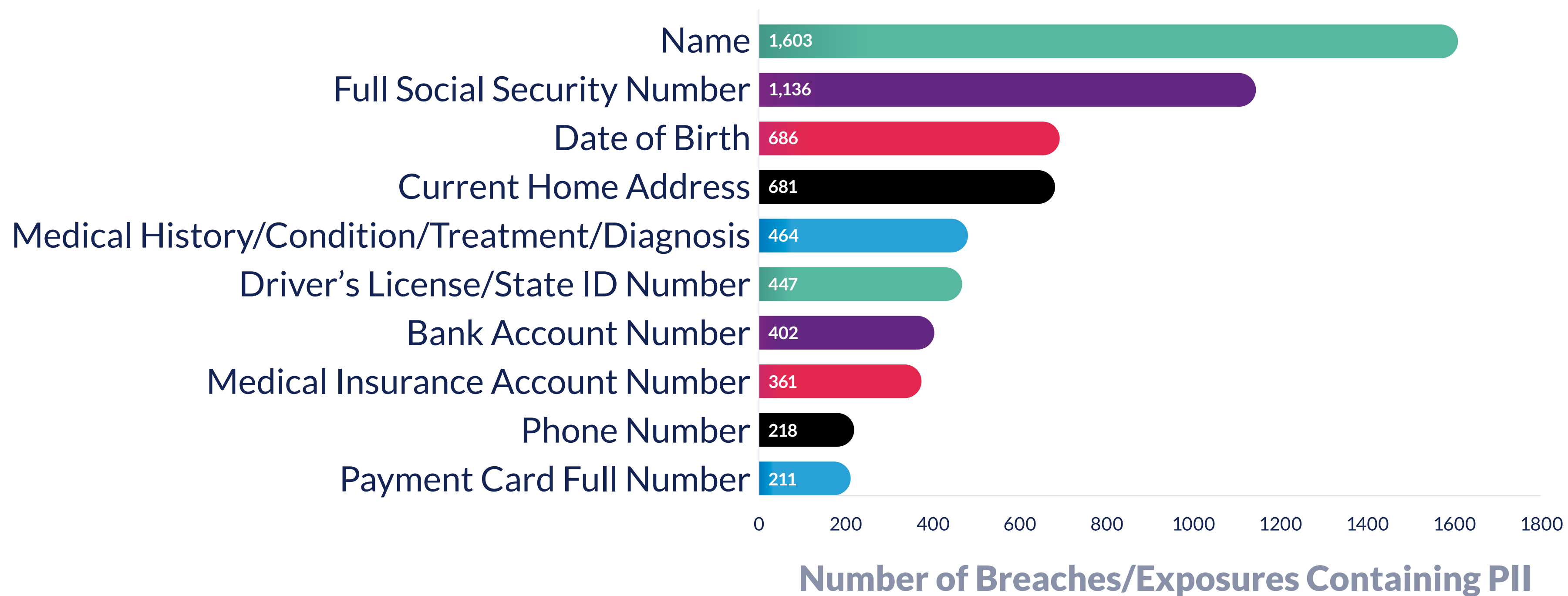


Compromises Involving Sensitive Records

● compromises - vs - ● sensitive records exposed



2021 Top 10 Breached Data Attributes

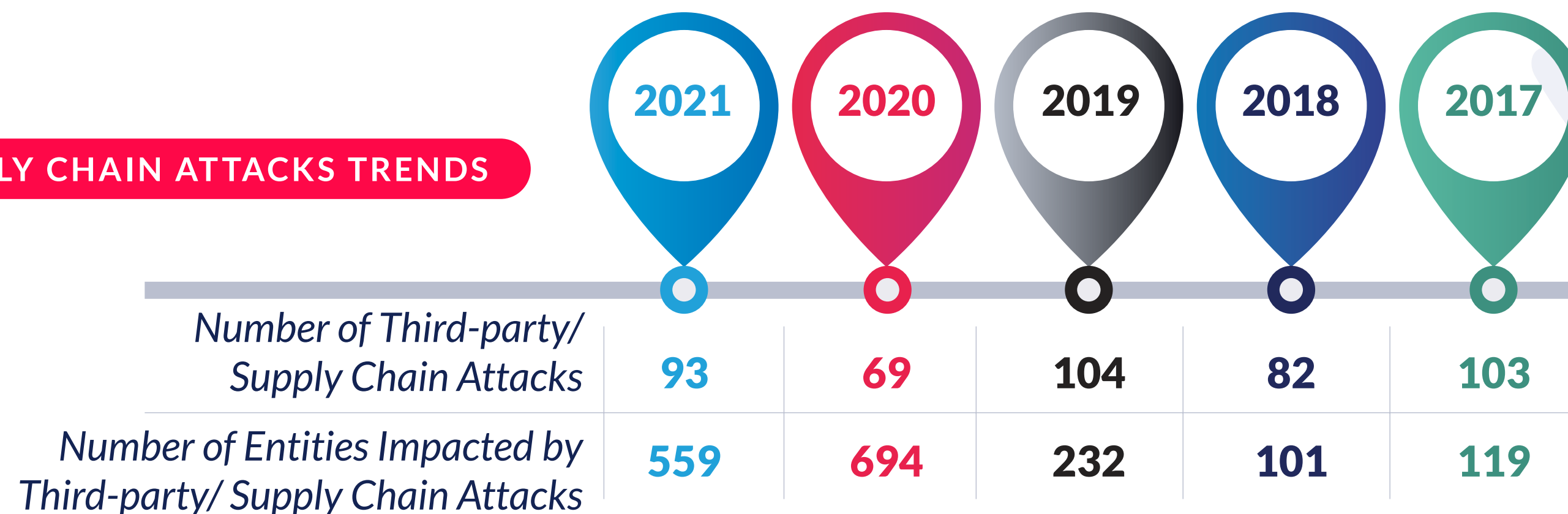


ALL DATA ATTRIBUTES

Name	1,603	Bank Account Routing Number	90	Friends/Family	6	Hometown	n/a
Full Social Security Number	1,136	Income/Wages/Earnings/Compensation	39	Employer Site/System Access Credentials	6	Personal Email Account Credentials	n/a
Date of Birth	686	Other Account Credentials	39	Financial Account PIN	6	Voter Registration Info/Preferences/Etc.	n/a
Current Home Address	681	Work Email Address	30	Insurance Account Details or Credentials	5	Work Email Account Credentials	n/a
Medical History/Condition/Treatment/Diagnosis	464	Employee ID Number/Credentials/Position/Etc.	24	Loan Account Details or Credentials	5	Web History/Preferences	n/a
Driver's License/State ID Number	447	Student ID Number/Student Login/Student Details	21	Merchant Login	5	Credit Dispute Info	n/a
Bank Account Number	402	Employer Contact Information	16	Bank Account Login Credentials	4	Non-Debit Payment Account Credentials	n/a
Medical Insurance Account Number	361	Employer Name	15	Phone Account Credentials	4		
Phone Number	218	Medical Provider Login Credentials	15	Prior Home Address	3		
Payment Card Full Number	211	Medical Insurance Account Credentials	14	Education	3		
Undisclosed Records	205	Payment Card Partial Number	13	W2 Other Info	3		
Personal Email Address	205	Partial Social Security Number	13	Location	2		
Medical Provider Account Number/Medical Record Number	198	Biometric/Authentication Data	12	Utility Account Number	2		
Payment Cardholder Name	177	Other Biographical	12	Social Media Login Credentials	1		
Payment Card Expiration Date	175	IP Address/Device ID	12	Utility Account Credentials	1		
Payment Card Security Code	170	Tax ID Number	9	Security Clearance/Access	n/a		
Passport Number/Visitor Status/Green Card	118	Investment Account Details or Credentials	7	Affiliations	n/a		

Supply Chain Attack Data 2017 through 2021

SUPPLY CHAIN ATTACKS TRENDS



	2021	2020	2019	2018	2017
Number of Third-party/ Supply Chain Attacks	93	69	104	82	103
Number of Entities Impacted by Third-party/ Supply Chain Attacks	559	694	232	101	119

NOTEWORTHY SUPPLY CHAIN ATTACKS

(All data was recorded by ITRC as of 1/6/2022)

- + **Blackbaud (2020):** 122 entities with 254,029 individual victims reported in 2021 in addition to the 480 entities with 12,561,072 individual victims of reported in 2020. The total number of entities is 602, with 12,815,101 individual victims
- + **CaptureRX:** 162 entities impacted
- + **Accellion:** 38 entities impacted
- + **Netgain Technologies, LLC (2020):** 24 entities impacted
- + **ParkMobile:** 19 entities impacted
- + **Automatic Funds Transfer Services, Inc.:** 14 entities impacted
- + **Elekta, Inc.:** 13 entities impacted
- + **Herff Jones:** 12 entities impacted
- + **North American Dental Management:** 11 entities impacted
- + **Vertafore:** 6 entities impacted
- + **Med-Data:** 6 entities impacted

Notable Trends

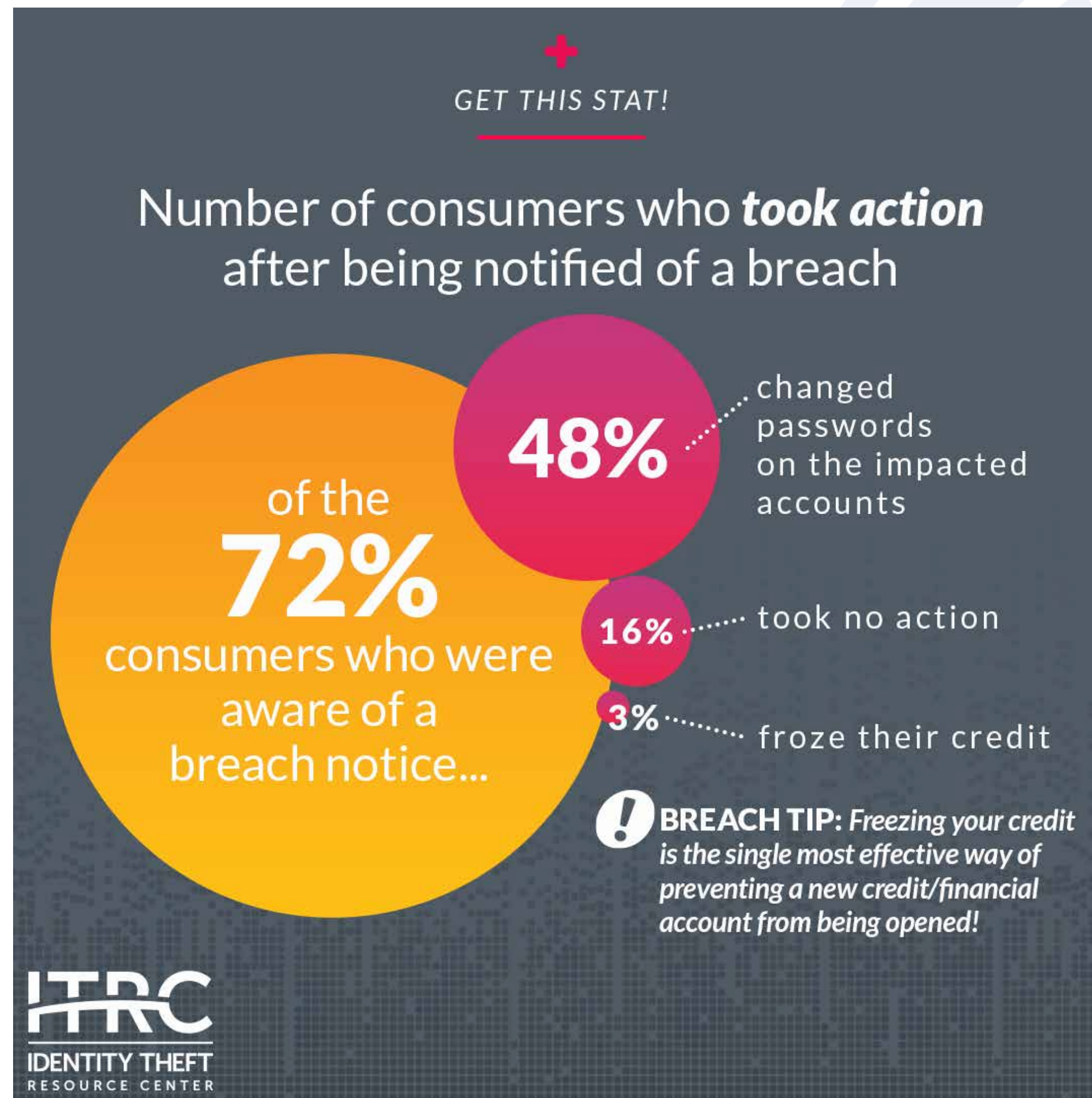
Breach notice transparency is decreasing

+ Why this is important: The lack of actionable information in breach notices prevents consumers from effectively judging the risks they face of identity misuse and taking the appropriate actions to protect themselves. A decrease in timely notices posted by states, including one state that updated breach notices in December 2021 for the first time since the Fall of 2020, also prevents consumers from taking action to protect themselves and organizations that assist identity crime victims from offering timely, effective advice.



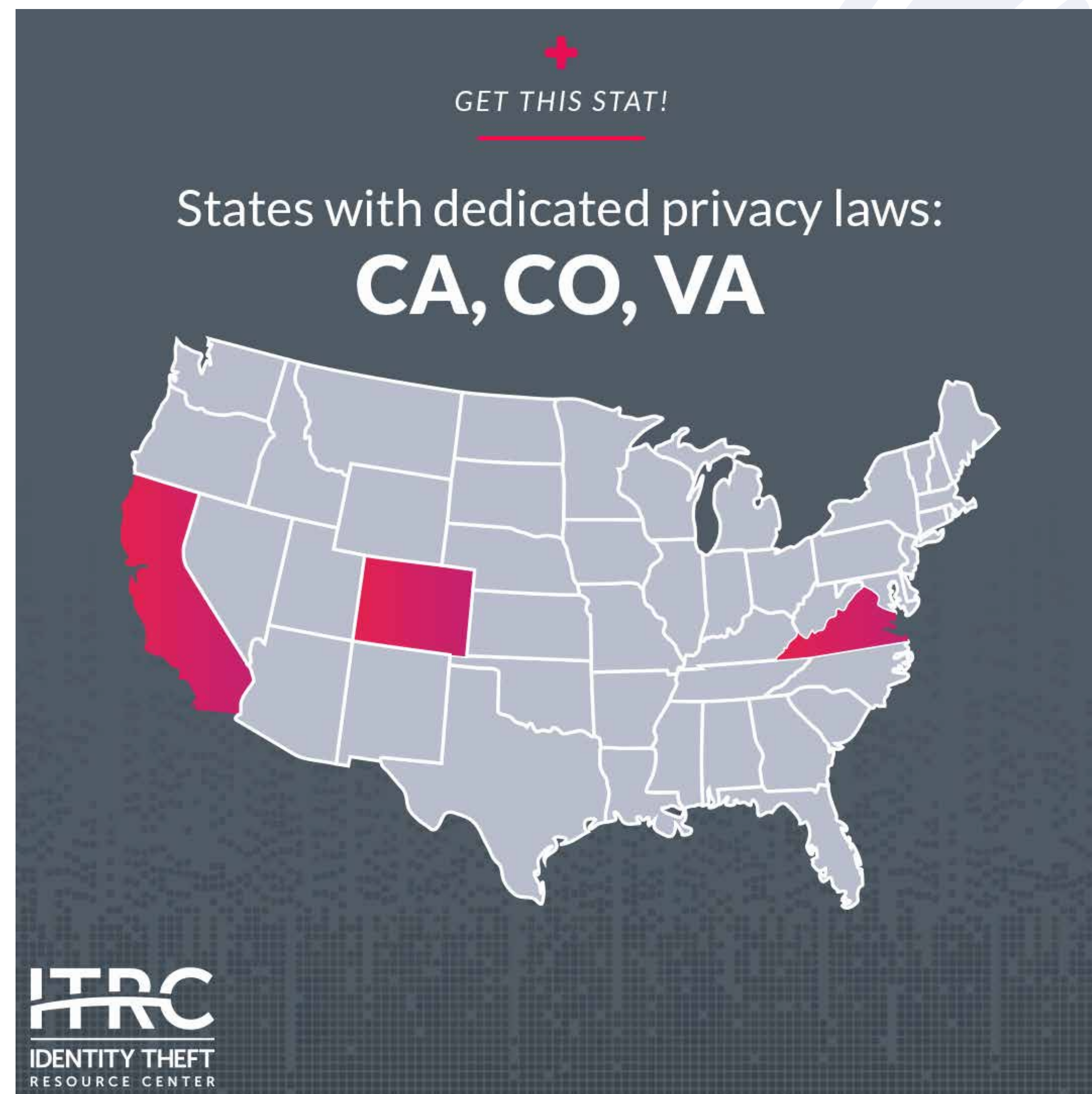
Notice effectiveness is low.

+ Why this is important: The form and substance of existing notices fail to prompt breach victims into taking actions that can significantly reduce the risk of their compromised identity information being misused.



New state privacy laws are helpful, but still result in **different victim protections** depending on where you live.

+ Why this is important: Every state defines personal information differently and every state has a different standard for if, when, and how a victim is notified that their information has been compromised. That means residents of one state may get a data breach notice when a resident across the border in a neighboring state may not receive an alert for the same data breach.



Case Studies

- A. Supply Chain Attack
– Accellion**
- B. Social Engineering
– Robinhood**
- C. Vulnerable Security
– T-Mobile**



Accellion

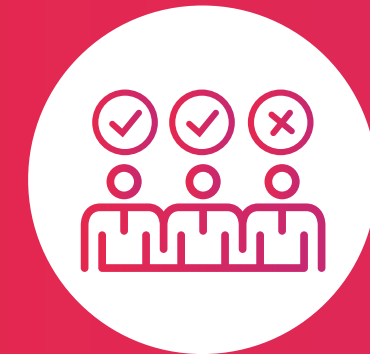
BREACH CAUSE: SUPPLY CHAIN ATTACK

An increasingly common attack method used by cybercriminals is known as a Supply Chain attack. Threat actors attack a single company that is part of a larger supply chain to access the information of multiple organizations.

In the case of Accellion, a U.S.-based software provider, cybercriminals targeted users of the company's 20-year old file sharing software. Accellion customers included law firms and cybersecurity companies that used the software to access sensitive client information that was compromised by ransomware gangs and cyber thieves. The cyberattacks targeted known flaws in Accellion software after the company alerted customers to a series of recently discovered vulnerabilities.

38 customers impacted
6,758,979 consumers at risk

Protect yourself:



Upgrade or Replace Legacy Software



Improve Vendor Compliance

BUSINESSES: *Cyberattacks seek to take advantage of weak or vulnerable security to gain access to the valuable data of multiple companies with a single attack. If you are a business leader, make sure your vendors' and partners' security is as good as your own.*

Robinhood

BREACH CAUSE: SOCIAL ENGINEERING

Social engineering attacks rely on individuals to share confidential information about themselves or their workplace. For example, ransomware operators manipulated a Robinhood customer service representative into giving a criminal access to the investment platform's customer support system.

7+ Million account holders impacted

Protect yourself:



Zero Trust Access model and updated processes

BUSINESSES: Consider adopting a Zero Trust Access model for giving employees and customers access to information, especially sensitive personal information. That means implementing “never trust, always verify” processes.

T-Mobile

BREACH CAUSE: VULNERABLE SECURITY

T-Mobile, one of the largest U.S. mobile telecommunications companies, has acknowledged six data breaches since 2018, including two in the last six months of 2021. In August 2021, T-Mobile's systems were attacked through an unprotected network access device in July. By August, the attacker had gained direct access to servers containing account and personal information on current, former, and prospective account holders. T-Mobile confirmed an additional compromise in late December 2021 that impacted an undisclosed number of customers.

53+ Million account holders impacted

Protect yourself:



Patching software flaws as soon as notified

BUSINESSES: Make sure the security on your internet accessible devices is configured correctly with up-to-date patches to avoid security and data breaches.



Use multi-factor authentication (MFA) when possible

CONSUMERS: Make sure you use multi-factor authentication with an authentication app when possible rather than having a code sent to your phone.

ITRC Breach Alert Service

Free Breach Alerts Coming Soon!

CONSUMER SERVICES

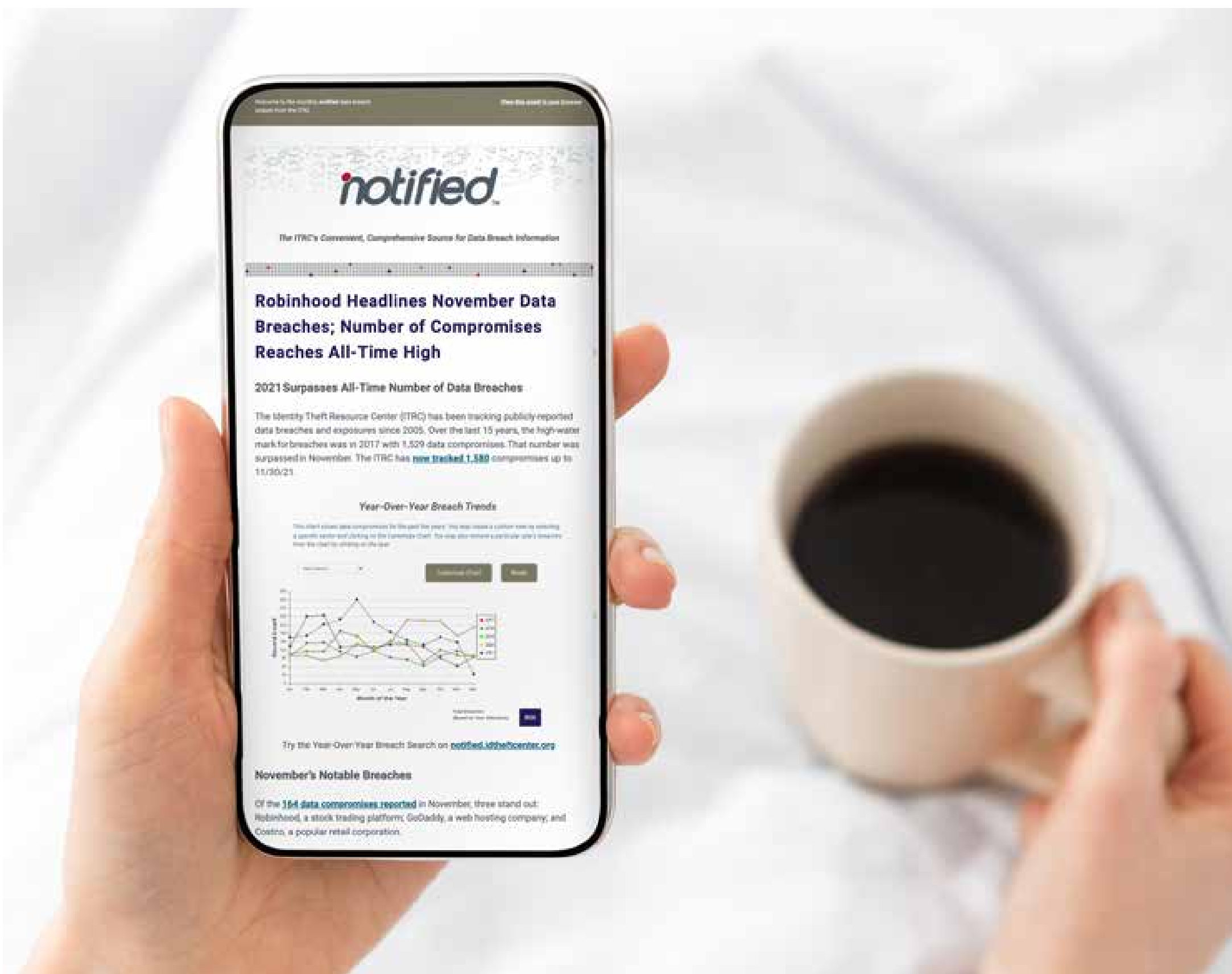
notifiedTM

Later in Q1, 2022, the ITRC will launch a free, data breach alert service for consumers where individuals can create a limited list of companies where they do business. If an organization on the list is added to the ITRC's **notified**TM data compromise database, a subscriber will receive an email alert.

Details in data breach notices are decreasing while the number of data breach announcements issued by website posts and news releases is increasing. As a result, consumers may not receive a direct notification of a data breach with actionable information so they can take steps to protect themselves.

To receive information on how to subscribe to the **notified** Consumer Breach Alert Service when it's available, sign-up for our monthly newsletter. We'll publish details on the new service in upcoming newsletters.

Register Today to Get **notified**TM



Breach Tracking for Risk Assessment!

BUSINESS SERVICES



The ITRC launched our *notified* data compromise tracking tool in 2020 as a free service to consumers and as a batch or subscription service for businesses. *notified* helps people and organizations assess the risks associated with data breaches, exposures, and leaks.

A paid Breach Alert Service subscription for businesses seeking to comply with new corporate and government cybersecurity and vendor due diligence requirements will be available later in 2022. For more information about *notified*'s business services, contact us at notifiedbyITRC@idtheftcenter.org.

Want More Data?

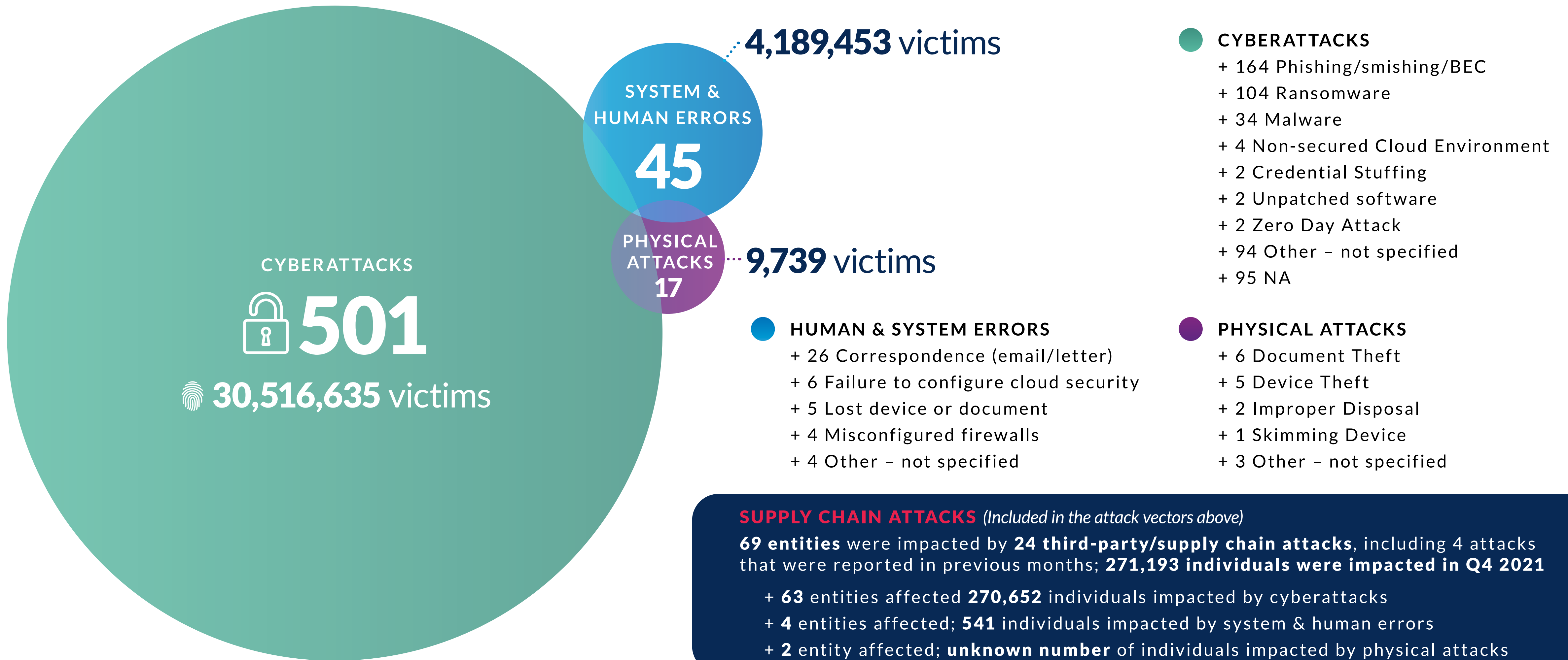
Contact Us to Upgrade Your Subscription Today!

Create your custom chart like the one below!

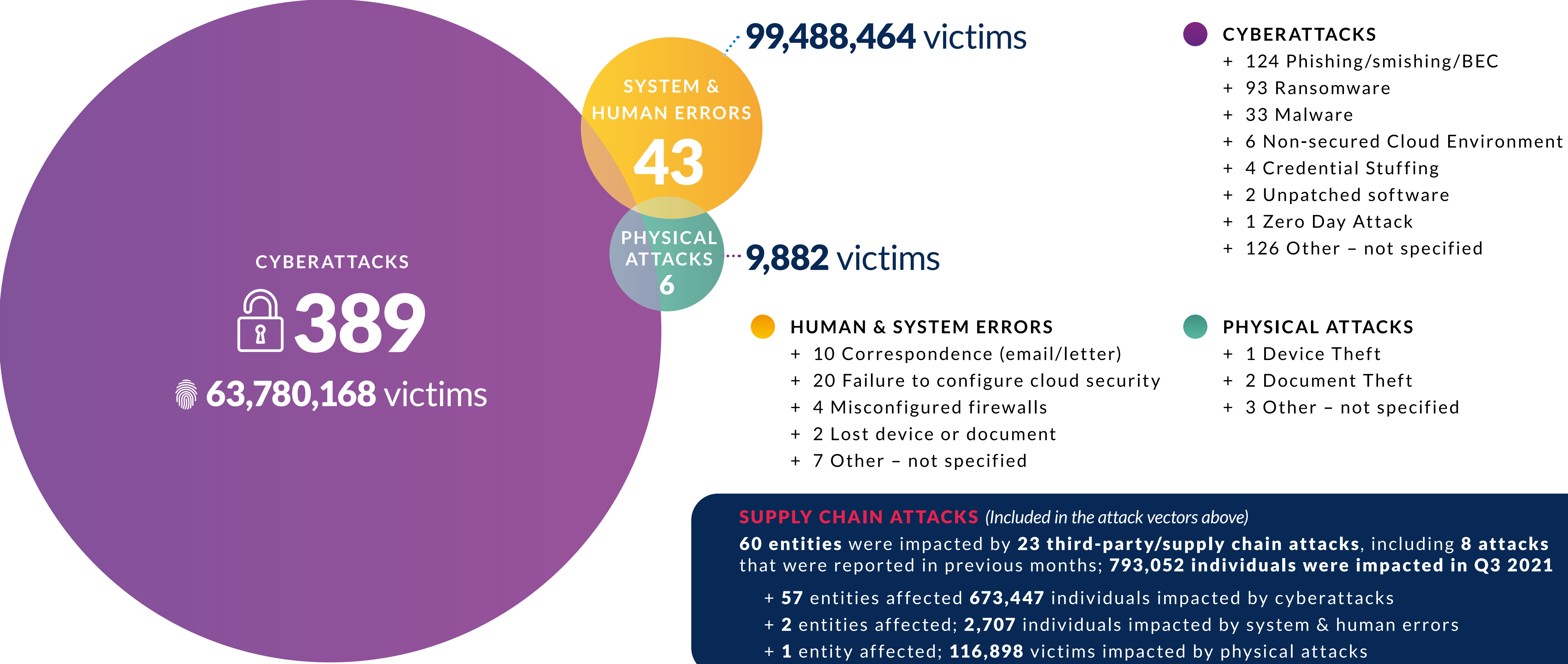


Appendix

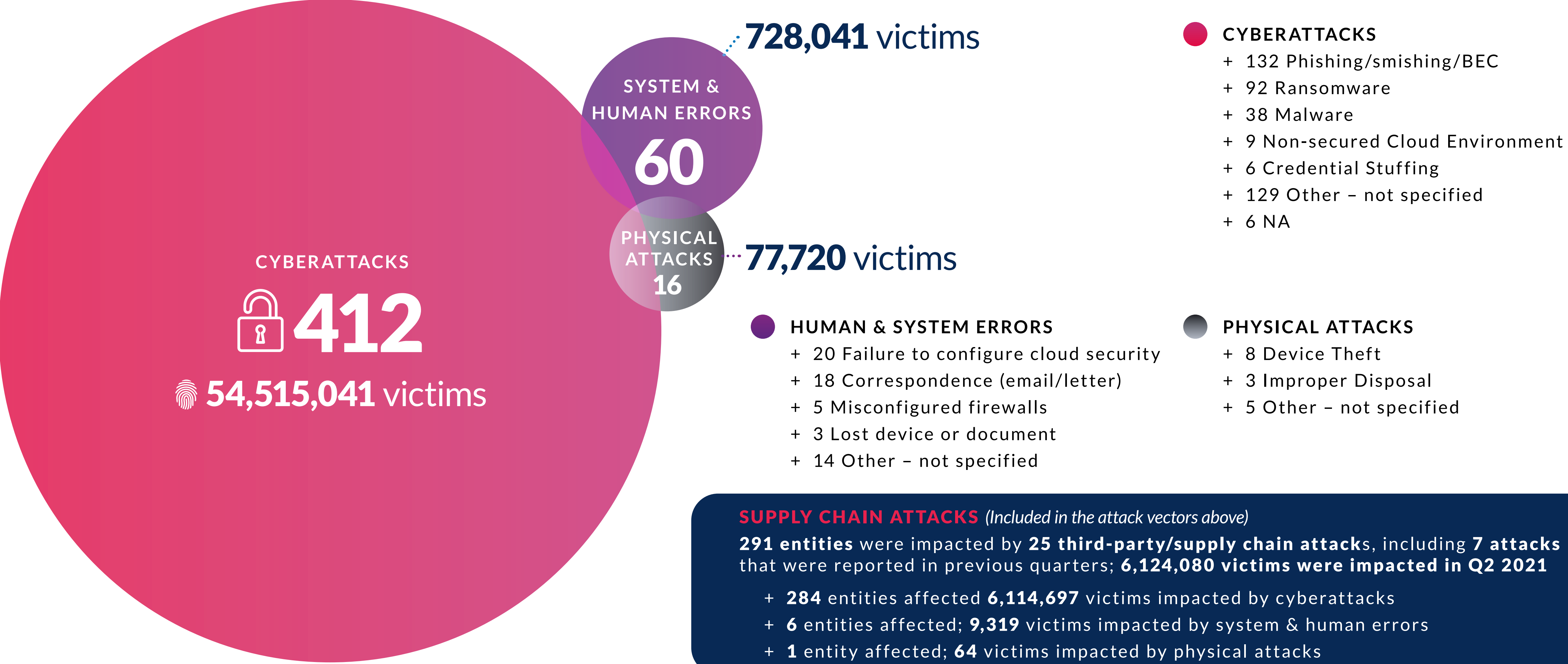
Data Breaches/Exposures Q4



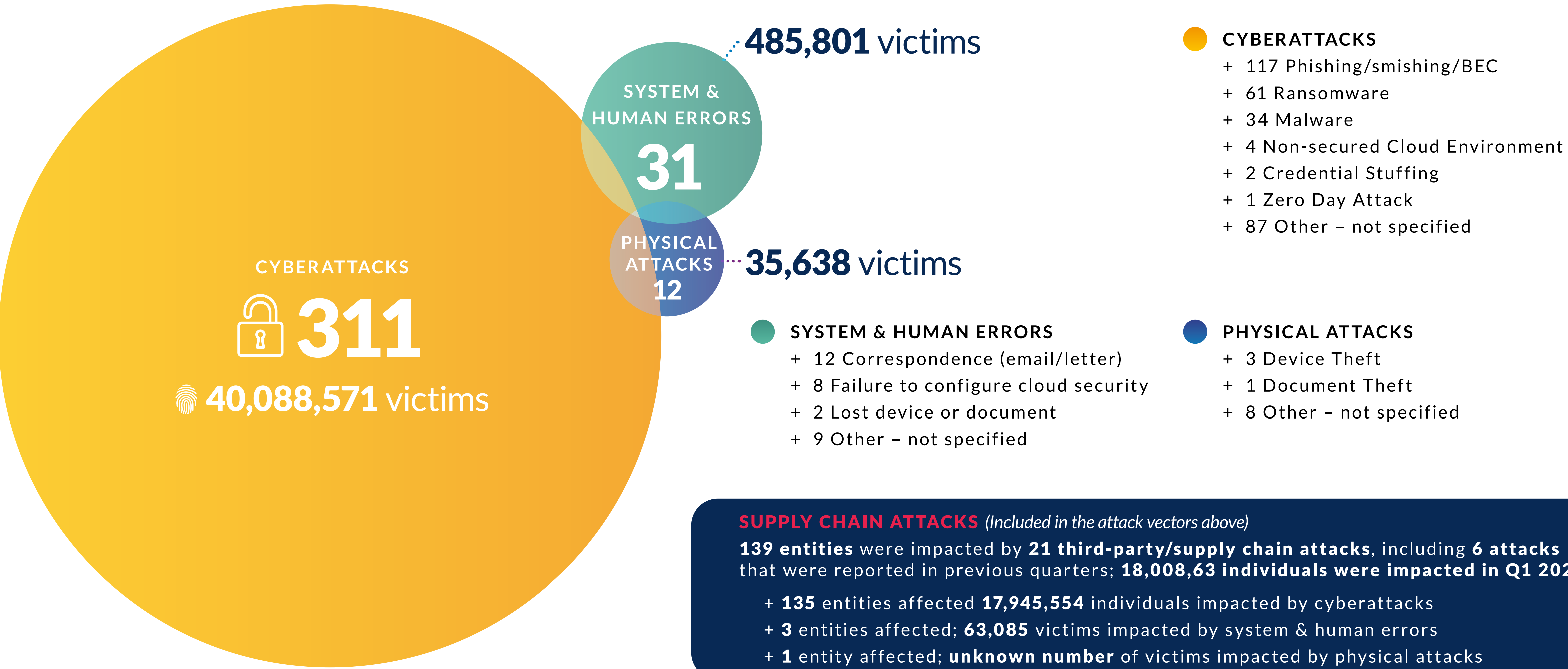
Data Breaches/Exposures Q3



Data Breaches/Exposures Q2



Data Breaches/Exposures Q1



Glossary of Terms

For purposes of this report the ITRC uses standard industry terms as defined by the National Institute of Standards & Technology (NIST) as well as specific definitions developed by the ITRC.

- + **Data Compromise** – The overall term used to refer to events where personal information is accessible by unauthorized individuals and/or for unintended purposes. This includes data breaches, data exposures, and data leaks.
- + **Data Breach** – When unauthorized individuals access and/or remove personal information from the place where it is stored.
- + **Data Exposure** - When personal information is available for access and/or removal from place where it is stored, but there is no evidence the information has been accessed by unauthorized individuals. This typically involves cloud-based data storage where cybersecurity protections are incorrectly configured or have not been applied.

+ **Data Leak** - In 2021 the ITRC added a new category of data compromise: Data Leaks. Leaks involve personal information that is publicly available or willingly shared on social media and represents no or low risk when viewed as individual records; however, when aggregated, the sheer volume of personal information available in a single database creates risk to the data subjects and value for identity criminals who specialize in social engineering and phishing. When these databases are left unprotected or otherwise made publicly available, the ITRC classifies these events as Data Leaks.

- + **Identity Crimes** – The overall term for a wide variety of state and federal criminal acts that are related to the theft and/or misuse of personal information.
- + **Identity Theft** – Taking personally identifiable information (PII) as protected by state or federal laws.
- + **Identity Fraud** – Using stolen personally identifiable information (PII).

Data Sources & Methodology

The ITRC gathers information about publicly reported data breaches from a variety of sources including: company announcements, mainstream news media, government agencies, recognized security research firms and researchers, and non-profit organizations. The ITRC accepts these reports “as is” and makes no warranty as to their accuracy or completeness.

It is common for the number of individuals impacted to change over time. Initial reports are often based on incomplete or inaccurate information resulting in the number of impacted individuals and the root cause of the data breach, among other factors, to require occasional updates.

Different states have different reporting requirements. This often results in lags between the time a government official is notified of a data breach and when the breach is officially reported. There are also variations in how data breaches are defined and what data is governed under a given state’s laws, resulting in data being subject to a breach notice in some states, but not in all.

There are a number of for-profit and non-profit organizations that publish data breach information, but each organization captures and views the information differently. There are four key differences in how the ITRC reports data breach information:

- + The ITRC tracks three distinct categories of data compromise. See our [Glossary of Terms](#) to learn more.
- + The ITRC only publishes data related to publicly reported U.S. compromises.
- + The ITRC focuses on the number of individuals impacted, not the number of records exposed in keeping with our mission of a victim assistance organization.
- + We do not report data breaches where the information is not protected under a state’s data breach notice law. For example, business records or intellectual property are generally excluded from state data breach laws.

2021 in review

Data Breach

ANNUAL REPORT

Identity Compromises: From the Era of Identity Theft to the Age of Identity Fraud

Consumer & Business Resources

For more information about low-cost identity education, protection, and recovery services for small businesses as well as the free services and education opportunities for consumers, visit idtheftcenter.org or by email at notifiedbyITRC@idtheftcenter.org.

The Identity Theft Resource Center is a 501(c)3 non-profit that does not endorse any particular company, product, or service.



idtheftcenter.org • 1-888-400-5530

The 2021 Data Breach Report is supported by:



Exhibit 3



Portfolio Media, Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FBI, Secret Service Warn Of Targeted Ransomware

By **Ben Kochman**

Law360, New York (November 18, 2019, 9:44 PM EST) -- Senior FBI and U.S. Secret Service officials said Monday that cybercriminals are increasingly using ransomware to target vulnerable entities like hospitals and municipalities, and urged victims to report attacks to authorities regardless of whether they capitulate and pay ransoms.

"We don't necessarily have the data that shows that the incidents of ransomware are rising, but what we do see is that those incidents are more targeted against victims that have the highest incentive to pay," said Tonya Ugoretz, deputy assistant director at the FBI's Cyber Division, during a panel at NYU's Center for Cybersecurity.

The ransom amounts being requested on average are rising, Ugoretz added Monday. Ransomware victims **often cave** to their attackers' demands, industry attorneys have told Law360, despite the FBI's official guidance that doing so could embolden cybercriminals to launch more attacks and incentivize others to try their hand at cybercrime.

Victims have included the city of Atlanta, which has said that it ended up spending more than \$10 million to **recover from** a cyberattack. Riviera Beach and Lake City in Florida have said that they paid \$600,000 and \$500,000 in bitcoin, respectively, this summer after failing to recover their data on their own.

Entities like smaller municipalities and hospitals are attractive to ransomware criminals, cybersecurity experts say, because they often have lesser IT defenses and a high incentive to regain access to their data quickly.

The bureau softened its stance on ransomware payments somewhat last month, writing in updated guidance that the FBI "understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers."

Michael D'Ambrosio, assistant director of the office of investigations at the Secret Service, which also investigates ransomware attacks, acknowledged on Monday that a blanket ban on entities paying ransoms is unrealistic.

"Law enforcement right now is not going to come out and say you cannot pay ransomware," he said during the panel. "However, it seems to be that you would want to do it in conjunction with law enforcement in order to try to find the individuals that have perpetrated the crime."

"There may be some information in there that we may be able to help you with," D'Ambrosio added, saying that in some cases the government has been able to help victims track down decryption keys and reclaim their data.

Ugoretz also urged ransomware victims to cooperate with federal authorities, who say they have been successful in tracking down ransomware attackers, even if it can be difficult to extradite the attackers to U.S. courts. For example, a federal investigation led to the **December indictment** of two Iranian men for the Atlanta attack, which court papers say was part of an international scheme in which the duo extorted dozens of hospitals, cities and public institutions.

Companies who invite the FBI into their systems to investigate suspected ransomware will be treated as victims, Ugoretz said, in an attempt to assuage fears that the bureau's agents, once granted access, could start looking around for potential evidence of corporate wrongdoing.

"We're not there on a fishing expedition," Ugoretz said. "We're not there to run in with green jackets and make a very noisy response ... We have a long history of treating victims like victims."

Ugoretz also defended the Justice Department's recent trend of so-called "name-and-shame" indictments, which target **alleged cybercriminals** based in countries like China, Russia and Iran, with whom the U.S. does not have extradition agreements.

U.S. authorities do sometimes find a way to extradite such defendants, Ugoretz said, pointing to recent cases including last week's appearance of 29-year-old Russian national Aleksei Burkov in Virginia federal court, where he is charged with operating a payment card fraud ring. Such indictments are key in sending a message to the rest of the world about what types of cybercrime the U.S. finds unacceptable, Ugoretz added.

"We talk a lot about norms in cyberspace," she said during the panel, "and these indictments are one way of signaling what is counternormative behavior."

--Editing by Daniel King.

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Atlanta Women's Health Group Data Breach Lawsuit Says OB/GYN Practice Waited 10 Mos. to Notify Victims](#)
