

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN**

PHILIP HODGSON, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

**KOVO+ (USA), INC. and ST. LOUIS
BEHAVIORAL MEDICINE INSTITUTE,
INC.,**

Defendant.

Case No.: 26-cv-993

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Philip Hodgson (“Plaintiff”), on behalf of all others similarly situated, by and through his undersigned counsel, brings this Class Action Complaint against Defendants Kovo + (USA), Inc. (“Kovo+”) and St. Louis Behavioral Medicine Institute, Inc. (“SLBMI”, collectively “Defendants”) and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiff and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendants with sensitive Personally Identifiable Information (“PII”)¹ and Protected Health Information (“PHI”) (collectively “Private Information”) that was impacted in a data breach (the “Data Breach” or the “Breach”).

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff's claims arise from each Defendant's respective failures to properly secure and safeguard Private Information that was entrusted to them, and their accompanying responsibility to store and transfer that information.

3. Defendant Kovo+ is a healthcare technology and AI process automation company that provides medical billing and revenue cycle management services to healthcare providers and medical billing firms² ("Defendant's Clients" or "Clients"), including Defendant SLBMI.

4. Defendant SLBMI is a behavioral healthcare that serves the St. Louis Metropolitan Area with behavioral health treatment and speciality programs for mental and emotional issues, and is one of Defendant Kovo+'s Clients.³

5. Each Defendant independently had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

6. On or about September 5 2026, notorious ransomware cybercriminal group "Pear" claimed responsibility for executing a successful cyberattack against Defendant Kovo+'s network and systems ("Data Breach").⁴ The Private Information exfiltrated in the Data Breach includes, upon information and belief and due to the nature of the services that Defendants provide, sensitive PII and PHI.

7. Defendants failed to take precautions designed to keep individuals' Private Information secure.

8. Each Defendant independently owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendants solicited, collected, used, and derived a benefit from the

² <https://kovoplus.com/about/> (last visited Oct. 1, 2026).

³ <https://slbmi.com/about-us/> (last visited Oct. 1, 2026)

⁴ <https://socradar.io/blog/data-breach/kovo-healthtech-corp-pear-ransomware-2026/> (last visited Oct. 1, 2026).

Private Information, yet breached their duty by failing to implement or maintain adequate security practices.

9. The sensitive nature of the data exposed through the Data Breach signifies that Plaintiff and Class Members have suffered irreparable harm. Plaintiff and Class Members have lost the ability to control their private information and are subject to an increased risk of identity theft.

10. Each Defendant independently failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information they maintained for Plaintiff and Class Members, causing the exposure of Plaintiff's and Class Members' Private Information.

11. As a result of Defendants inadequate digital security and notice process, Plaintiff's and Class Members' Private Information was exposed to criminals. Plaintiff and the Class Members have suffered and will continue to suffer injuries including: financial losses caused by misuse of their Private Information; the loss or diminished value of their Private Information as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

12. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendants failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendants inadequate information security practices; (iii) effectively secure hardware containing protected Private Information using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiff and Class Members of the Data Breach. Defendants conduct amounts to at least negligence and violates federal and state statutes.

13. Plaintiff brings this action individually and on behalf of a Class of similarly situated individuals against Defendants for: negligence; negligence *per se*; unjust enrichment, breach of third party beneficiary contract, and breach of implied contract.

14. Plaintiff seeks to remedy these harms and prevent any future data compromise on

behalf of himself, and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants inadequate data security practices.

PARTIES

Plaintiff

15. Plaintiff is a citizen and resident of Perryville, Missouri.

Defendants

16. Defendant Kovo+ is a corporation that maintains its principal place of business at 1235 Menomonie St Ste B, Eau Claire, Wisconsin 54703. Defendant Kovo+'s registered agent is Incorp Services, Inc. located at 1500 N Grant St Ste B, Denver, Colorado 80203.

17. Defendant SLBMI is a corporation that maintains its principal place of business at 1129 Macklind Ave, Saint Louis, Missouri 63110-1440. Defendant SLBMI's registered agent is CSC-Lawyers Incorporating Service Company located at 221 Bolivar St, Jefferson City, Missouri 65101.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendants citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A).

19. This Court has personal jurisdiction over Defendants because Defendant Kovo+ is registered to do business and maintains its principal place of business in this District.

20. Venue is proper in this Court because Defendant Kovo+'s principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Background on Defendants

21. Defendant Kovo+ is a healthcare technology and AI process automation company that provides medical billing and revenue cycle management services to healthcare providers and medical billing firms⁵, including Defendant SLBMI.

22. Defendant SLBMI is a behavioral healthcare that serves the St. Louis Metropolitan Area with behavioral health treatment and speciality programs for mental and emotional issues.⁶

23. Upon information and belief, each Defendant independently made promises and representations to individuals, including Plaintiff and Class Members, that the Private Information collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.

24. Plaintiff and Class Members provided their Private Information to Defendants, either directly or indirectly, with the reasonable expectation and on the mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

25. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, each Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff and the Class Members' Private Information from disclosure to third parties.

B. The Data Breach

26. On or about September 5 2026, notorious ransomware cybercriminal group "Pear" claimed responsibility for executing a successful cyberattack against Defendant Kovo+'s network and systems ("Data Breach").⁷ The Private Information exfiltrated in the Data Breach includes,

⁵ <https://kovoplus.com/about/> (last visited Oct. 1, 2026).

⁶ <https://slbmi.com/about-us/> (last visited Oct. 1, 2026)

⁷ <https://socradar.io/blog/data-breach/kovo-healthtech-corp-pear-ransomware-2026/> (last visited Oct. 1, 2026).

upon information and belief and due to the nature of the services that Defendants provide, sensitive PII and PHI.

27. Defendants failed to take precautions designed to keep individuals' Private Information secure.

28. While Defendants sought to minimize the damage caused by the Data Breach, they cannot and have not denied that there was unauthorized access to the sensitive Private Information of Plaintiff and Class Members.

29. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendants Failure to Prevent, Identify, and Timely Report the Data Breach

30. The Private Information that Defendants allowed to be exposed in the Data Breach are the types of private information that Defendants knew or should have known would be the target of cyberattacks.

31. Despite their own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,⁸ Defendants failed to disclose that their systems and security practices, or those of third-party vendors, were inadequate to reasonably safeguard individuals' Private Information.

32. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.⁹ Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

D. Defendants Fail to Comply with FTC Guidelines

33. The FTC has promulgated numerous guides for businesses that highlight the

⁸ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business>. (last visited Oct. 1, 2026).

⁹ *Id.*

importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.¹⁰

35. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹¹

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

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

¹⁰ Protecting Personal Information: A Guide for Business, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 1, 2026).

¹¹ *Id.*

38. These FTC enforcement actions include actions against healthcare entities that fail to adequately protect patient's data, like Defendants. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

39. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants duty in this regard.

40. Defendants failed to properly implement basic data security practices.

41. Defendants’ failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals’ Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

42. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of individuals; Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Cherry

E. Defendants Fail to Comply with HIPAA Guidelines

43. Defendants are covered businesses under HIPAA (45 C.F.R. § 160.102) and are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E (“Standards for Privacy of Individually Identifiable Health Information”), and Security Rule (“Security Standards for the Protection of Electronic Protected Health

Information”), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

44. Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act (“HITECH”).¹² See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

45. HIPAA’s *Privacy Rule or Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

46. HIPAA’s *Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

47. HIPAA requires “compl[iance] with the applicable standards, implementation specifications, and requirements” of HIPAA “with respect to electronic protected health information.” 45 C.F.R. § 164.302.

48. “Electronic protected health information” is “individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R. § 160.103.

49. HIPAA’s Security Rule requires Defendants to do the following:

- a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
- d. Ensure compliance by their workforce.

¹² HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

50. HIPAA also requires Defendants to “review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendants are required under HIPAA 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.” 45 C.F.R. § 164.312(a)(1).

51. HIPAA and HITECH also obligate Defendants to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

52. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

53. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

54. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule

Guidance Material.¹³ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good business practices with respect to standards for securing e-PHI.” US Department of Health & Human Services, Guidance on Risk Analysis.¹⁴

F. Defendants Fail to Comply with Industry Standards

55. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

56. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

57. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

58. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST

¹³ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last visited Oct. 1, 2026).

¹⁴ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last visited Oct. 1, 2026).

Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

59. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

60. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁵

61. To prevent and detect cyber-attacks and/or ransomware attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- d. Configure firewalls to block access to known malicious IP addresses.
- e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- f. Set anti-virus and anti-malware programs to conduct regular scans automatically.
- g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and

¹⁵ How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

those with a need for administrator accounts should only use them when necessary.

- h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- m. Execute operating system environments or specific programs in a virtualized environment.
- n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁶

62. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

¹⁶ *Id.* at 3-4.

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] for Office[Visual Basic for Applications].¹⁷

63. These foregoing frameworks are existing and applicable industry standards for a business and healthcare provider's obligations to provide adequate data security for individuals' sensitive information. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach

G. The Harm Caused by the Data Breach Now and Going Forward

64. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 17 C.F.R. § 248.201(9). When “identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open

¹⁷ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

new utility accounts, or get medical treatment on your health insurance.”¹⁸

65. The types of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

66. Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

67. Stolen Private Information is often trafficked on the “dark web,” a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the “dark web” due to this encryption, which allows users and criminals to conceal their identities and online activity.

68. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.¹⁹

69. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online “dark market”—in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person’s identity.”²⁰ Marketplaces similar to the now-defunct AlphaBay continue to be “awash with [PII] belonging to victims from countries all over the world.”²¹

70. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details

¹⁸ *Prevention and Preparedness*, New York State Police, <https://troopers.ny.gov/prevention-and-preparedness> (last visited Oct. 1, 2026).

¹⁹ *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) <https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring> (last visited Oct. 1, 2026).

²⁰ *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018), <https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/> (last visited Oct. 1, 2026).

²¹ *Id.*

have a price range of \$50 to \$200.²² Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²³

71. 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 in 2019, resulting in more than \$3.5 billion in losses to individuals and business victims.²⁴

72. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."²⁵ Defendants did not rapidly report to Plaintiff and Class Members that their Private Information had been stolen.

73. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendants Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendants with the mutual understanding that Defendants would safeguard their Private Information against theft and not allow access to and misuse of their

²² *Id.*

²³ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015) <https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Oct. 1, 2026).

²⁴ *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion> (last visited Oct. 1, 2026).

²⁵ *Id.*

personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further injurious breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff and Class Members' Private Information.

74. In addition to a remedy for economic harm, Plaintiff and Class Members maintain an interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

75. Defendants disregarded the rights of Plaintiff and Class Members by (a) intentionally, wilfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their network servers were protected against unauthorized intrusions; (b) failing to disclose that they did not have adequately robust security protocols and training practices in place to safeguard Plaintiff and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

76. The actual and adverse effects to Plaintiff and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by Defendants wrongful actions and/or inaction and the resulting Data Breach require Plaintiff and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiff and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

H. Plaintiff's Experience

77. Plaintiff is a patient of Defendant SLBMI.

78. As a condition of receiving medical services, Plaintiff was required to supply Defendants with his Private Information.

79. Defendants were in possession of Plaintiff's Private Information before, during and after the Data Breach.

80. Plaintiff reasonably understood and expected that Defendants would safeguard his Private Information and timely and adequately notify him in the event of a data breach. Plaintiff would not have allowed Defendants, or anyone in Defendants position, to maintain his Private Information if he believed that Defendants would fail to implement reasonable and industry standard practices to safeguard that information from unauthorized access.

81. Plaintiff greatly values his privacy and Private Information and takes reasonable steps to maintain the confidentiality of his Private Information. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

82. Plaintiff stores any and all documents containing Private Information in a secure location and destroys any documents he receives in the mail that contain any Private Information or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

83. To the best of Plaintiff's knowledge, his Private Information has not been compromised in a prior data breach.

84. As a result of the Data Breach, Plaintiff has spent considerable time researching the Data Breach, reviewing his bank accounts, monitoring his credit report, changing his passwords and other necessary mitigation efforts. This is valuable time that Plaintiff spent that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

85. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendants delay in noticing him of the fact Private Information was

acquired by criminals as a result of the Data Breach.

86. Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present and continued increased risk of identity theft and fraud for years to come.

87. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendants possession, is protected and safeguarded from future breaches.

88. As a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendants did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and likely published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendants obtained from Plaintiff; and (g) other economic and non-economic harm.

CLASS ALLEGATIONS

89. Plaintiff brings this class action, individually and on behalf of the following Nationwide Class:

All individuals whose Private Information was compromised as a result of the Data Breach (the “Nationwide Class”).

90. Specifically excluded from the Class are Defendants, their officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, servants, partners, joint venturers, or entities controlled by Defendants, and their, successors, assigns, or

other persons or entities related to or affiliated with Defendants and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

91. Plaintiff reserves the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

92. This action may be certified as a class action because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

93. Numerosity: The Members of the Class are so numerous that joinder of all of them is impracticable. Upon information and belief, the proposed Class includes thousands of members.

94. Typicality of Claims: Plaintiff's claims are typical of those of other Class Members because Plaintiff, like the unnamed Class, had his Private Information compromised as a result of the Data Breach. Plaintiff is a member of the Class, and his claims are typical of the claims of the members of the Class. The harm suffered by Plaintiff is similar to the harm suffered by all other Class Members, which was caused by the same misconduct by Defendants.

95. Adequacy of Representation: Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has no interests antagonistic to, nor in conflict with, the Class. Plaintiff has retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

96. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class Members are relatively small, the expense and burden of individual litigation make it impossible for individual Class Members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendants will likely continue their wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for their wrongdoing as asserted herein.

97. Predominant Common Questions: The claims of all Class Members present

common questions of law or fact, which predominate over any questions affecting only individual Class Members, including:

- a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- b. Whether Defendants data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- c. Whether Defendants storage of Plaintiff and Class Member's Private Information was done in a negligent manner;
- d. Whether Defendants had a duty to protect and safeguard Plaintiff and Class Members' Private Information;
- e. Whether Defendants' conduct was negligent;
- f. Whether Defendants conduct violated Plaintiff and Class Members' privacy;
- g. Whether Defendants conduct violated the statutes as set forth herein;
- h. Whether Defendants took sufficient steps to secure individuals' Private Information;
- i. Whether Defendants were unjustly enriched; and
- j. The nature of relief, including damages and equitable relief, to which Plaintiff and Class Members are entitled.

98. Information concerning Defendants policies are available from Defendants records.

99. Plaintiff knows of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a class action.

100. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendants. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

101. Given that Defendants have not indicated any changes to their conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at

law.

CAUSES OF ACTION
COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against Defendants)

102. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 101, as though fully set forth herein.

103. Plaintiff brings this claim individually and on behalf of the Class Members.

104. Defendants knowingly collected, came into possession of, and maintained Plaintiff and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

105. Each Defendant independently had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class Members' Private Information.

106. Each Defendant independently had, and continues to have, a duty to timely disclose that Plaintiff's and Class Members' Private Information within their possession was compromised and precisely the types of information that were compromised.

107. Each Defendant independently owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, HIPAA, and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected individuals' Private Information.

108. Each Defendant's independent duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and Class Members. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

109. Each Defendant's independent duty to use reasonable care in protecting

confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Private Information.

110. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff and Class Members' Private Information.

111. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff and Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems; and
- c. Failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

112. Each Defendant independently, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class Members' Private Information within Defendants possession.

113. Each Defendant independently, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class Members' Private Information.

114. Each Defendant independently, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendants possession might have been compromised and precisely the type of information compromised.

115. Each Defendant independently breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. §

45, Defendants failed to implement proper data security procedures to adequately and reasonably protect Plaintiff and Class Members' Private Information. In violation of the FTC guidelines, *inter alia*, Defendants did not protect the Private Information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

116. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiff and Class Members' Private Information would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

117. It was foreseeable that the failure to adequately safeguard Plaintiff and Class Members' Private Information would result in injuries to Plaintiff and Class Members.

118. Defendants' breach of duties owed to Plaintiff and Class Members caused Plaintiff and Class Members' Private Information to be compromised.

119. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their Private Information would not have been compromised.

120. As a result of Defendants' failure to timely notify Plaintiff and Class Members that their Private Information had been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

121. As a result of Defendants' negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiff and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort,

and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class Against Defendants)

122. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 101, as though fully set forth herein.

123. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect Plaintiff and Class Members’ Private Information. Various FTC publications and orders also form the basis of Defendants duty.

124. Each Defendant independently violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff and Class Members’ Private Information and by failing to comply with industry standards.

125. Defendants’ conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendants systems.

126. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

127. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

128. As a result of Defendants’ negligence *per se*, Plaintiff and Class Members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and

restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing, and correcting the current and future consequences of the Data Breach.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against Defendants)

129. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 101, as though fully set forth herein.

130. Plaintiff and Class Members conferred a benefit upon Defendants by providing Defendants with their Private Information.

131. Each Defendant independently appreciated or had knowledge of the benefits conferred upon themselves by Plaintiff. Each Defendant also benefited from the receipt of Plaintiff and Class Members' Private Information.

132. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class Members' Private Information because Defendants failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendants had they known Defendants would not adequately protect their Private Information.

133. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by them because of their misconduct and the Data Breach they caused.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant SLBMI)

134. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 101, as though fully set forth herein.

135. Plaintiff and the Class provided and entrusted their Private Information to Defendant SLBMI. Plaintiff and the Class provided their Private Information to Defendant SLBMI as part of its regular business practices.

136. In so doing, Plaintiff and the Class entered into implied contracts with Defendant SLBMI by which Defendant SLBMI agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant SLBMI. Implied in these exchanges was a promise by Defendant SLBMI to ensure that the Private Information of Plaintiff and Class Members in its possession was secure.

137. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant SLBMI with their Private Information. In exchange, Defendant SLBMI agreed to, among other things, and Plaintiff and the Class understood that Defendant SLBMI would: (1) provide services to Plaintiff and Class Members'; (2) take reasonable measures to protect the security and confidentiality of Plaintiff and Class Members' Private Information; and (3) protect Plaintiff and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

138. Implied in these exchanges was a promise by Defendant SLBMI to ensure the Private Information of Plaintiff and Class Members in their possession was only used to provide the agreed-upon reasons, and that Defendant SLBMI would take adequate measures to protect Plaintiff and Class Members' Private Information.

139. A material term of this contract is a covenant by Defendant SLBMI that it would take reasonable efforts to safeguard that information. Defendant SLBMI breached this covenant by allowing Plaintiff and Class Members' Private Information to be accessed in the Data Breach.

140. Indeed, implicit in the agreement between Defendant SLBMI and Plaintiff and Class Members was the obligation that both parties would maintain information confidentially and securely.

141. These exchanges constituted an agreement and meeting of the minds between the parties.

142. When the parties entered into an agreement, mutual assent occurred. Plaintiff and Class Members would not have disclosed their Private Information to Defendant SLBMI but for the prospect of utilizing Defendants services. Conversely, Defendant SLBMI presumably would not have taken Plaintiff and Class Members' Private Information if they did not intend to provide Plaintiff and Class Members with its services.

143. Defendant SLBMI was therefore required to reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure and use.

144. Plaintiff and Class Members would not have entrusted their Private Information to Defendant SLBMI in the absence of their implied contracts with Defendant SLBMI and would have instead retained the opportunity to control their Private Information.

145. Defendant SLBMI breached the implied contracts with Plaintiff and Class Members by failing to reasonably safeguard and protect Plaintiff and Class Members' Private Information.

146. Defendant SLBMI's failure to implement adequate measures to protect the Private Information of Plaintiff and Class Members violated the purpose of the agreement between the parties.

147. As a proximate and direct result of Defendant SLBMI breach of their implied contracts with Plaintiff and Class Members, Plaintiff and the Class Members suffered damages as

described in detail above.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant Kovo+ Care)

148. Plaintiff incorporates by reference and re-alleges each and every allegation set forth above in paragraphs 1 through 101, as though fully set forth herein.

149. Defendant Kovo+ entered into contracts, written or implied, with its Clients, including Defendant SLBMI, to perform services that include, but are not limited to, providing medical coding and risk adjustment services. Upon information and belief, these contracts are virtually identical between and among Defendant Kovo+ and its Clients around the country whose customers and patients, including Plaintiff and Class Members, were affected by the Data Breach.

150. In exchange, Defendant Kovo+ agreed, in part, to implement adequate security measures to safeguard the Private Information of Plaintiff and the Class.

151. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant Kovo+ and its Clients. Defendant Kovo+ knew that if it were to breach these contracts with its Clients, its Clients' patients—Plaintiff and Class Members—would be harmed.

152. Defendant Kovo+ breached the contracts it entered into with its Clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

153. Plaintiff and the Class were harmed by Defendant Kovo+'s breach of its contracts with its Clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendants, as follows:

- (a) For an order determining that this action is properly brought as a class action and certifying Plaintiff as the representative of the Class and his counsel as Class Counsel;
- (b) For an order declaring that Defendants conduct violates the laws referenced herein;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For damages in amounts to be determined by the Court and/or jury;
- (e) For an award of statutory damages or penalties to the extent available;
- (f) For pre-judgment interest on all amounts awarded;
- (g) For an order of restitution and all other forms of monetary relief; and
- (h) Such other and further relief as
- (i) the Court deems necessary and appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: October 1, 2026

/s/ Leanna Loginov
Leanna Loginov
SHAMIS & GENTILE, P.A.
14 NE First Avenue, Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
lloginov@shamisgentile.com

Steven Sukert*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: 954-525-4100
sukert@kolawyers.com

Attorneys for Plaintiff
**pro hac vice* forthcoming