

**IN THE COURT OF COMMON PLEAS
HAMILTON COUNTY, OHIO**

ROSE BOSHEARS, DERISHIA SMITH,
AND TOMMIE SHEARER individually and
on behalf of all others similarly situated,

Case No. A 2101886

Judge: Jennifer Branch

Plaintiff,

v.

TRIHEALTH, INC.

Defendant(s).

PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiffs ROSE BOSHEARS, DERISHIA SMITH, & TOMMIE SHEARER (“Plaintiffs”), bring this class action lawsuit on behalf of themselves and all other persons similarly situated, and for their First Amended Class Action Complaint against Defendant TRIHEALTH, INC. (“TriHealth”), allege with personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from Defendant’s failure to secure and protect Plaintiffs’ and Class Members’ Sensitive Information from unauthorized disclosure to criminal third parties. There are two types of Sensitive Information at issue in the case: (1) personal identifying information (“PII”), including names, email addresses, dates of births, and physical addresses; and (2) protected health information (“PHI”), including health related information and health insurance information. PII and PHI are collectively referred to herein as “Sensitive Information.”

2. Healthcare providers and their agents that collect and store Sensitive Information of their patients have statutory, regulatory, and common law duties to safeguard that information and ensure that it remains private.

3. Plaintiffs and class members are aware of a medical provider's duty of confidentiality, and as a result, have an objective reasonable expectation that TriHealth will not share or disclose, whether intentionally or unintentionally, PII or PHI, in the absence of authorization for any purpose that is not directly related to or beneficial to patient care.

4. Likewise, pursuant to HIPAA and industry standards, medical providers understand that part of the services they provide to patients includes confidentiality and the need to provide adequate data security procedures and protocols to protect the Sensitive Information.

5. Indeed, Defendant's patients, including Plaintiffs, entered into implied contracts with Defendant as part of their medical services whereby Plaintiffs and Class Members reasonably expected that the Sensitive Information they entrusted to Defendant would remain confidential and would be protected with adequate data security systems from foreseeable criminal third party cyber threats.

6. As described herein, Defendant breached its statutory, regulatory, common law and contractual duties by failing to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect patients' Sensitive Information.

7. As a result of Defendant's failure to implement and follow reasonable security procedures, the Sensitive Information is now in the possession of criminal networks placing Plaintiffs and the Class Members at substantially increased risk for identity theft presently and for years to come. Plaintiffs and Class Members have suffered numerous actual, concrete, and imminent injuries as a direct result of the Data Breach, including, but not limited to: (a) theft of

their Sensitive Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with the time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) the emotional distress, stress, nuisance, and annoyance of the responding to and resulting from the Data Breach; (e) the actual and/or imminent injury arising from the actual and/or potential fraud and identity theft posed by their Sensitive Information being placed in the hands of the ill-intentioned hackers and/or criminals; (f) damages to and diminution of value of their Sensitive Information entrusted to Defendant; (g) the actual damages in the difference between the services that should have been delivered and the services that were actually delivered; and (h) the continued risk to their Sensitive Information and personal identity, which requires further protection.

THE PARTIES

8. Plaintiff Rose Boshears is a natural person and a citizen of Ohio and a resident of Hamilton County, Ohio. Prior to the Data Breach, Ms. Boshears was a patient at a TriHealth facility and was careful with her PII and PHI. Upon information and belief, she provided her PII to TriHealth as a part of receiving medical services, including her social security number, date of birth, address, email address, and insurance information. She expected her PII and PHI to be secure and confidential and that TriHealth would implement adequate data security as part of the medical services. Plaintiff received a Notice Letter dated April 6, 2021 informing her that her PII and PHI that she had entrusted to Defendant had been compromised in a Data Breach. As a result of receiving the Notice Letter, Plaintiff has spent time reviewing her financial accounts and researching the impact of the Data Breach. She will be spending additional time reviewing her medical information for medical identity theft and continuing to monitor her financial accounts.

9. Plaintiff Derishia Smith is a natural person and citizen of Texas and resident of Dallas County, Texas. Prior to the Data Breach, Ms. Smith was a patient at a TriHealth facility and was careful with her PII and PHI. Upon information and belief, she provided her PII to TriHealth as a part of receiving medical services that included her social security number, date of birth, address, email address, and insurance information. She expected her PII and PHI to be secure and confidential and that TriHealth would implement adequate data security as part of the medical services. Plaintiff received a Notice Letter dated April 6, 2021 informing her that her PII and PHI that she had entrusted to Defendant had been compromised in a Data Breach. As a result of receiving the Notice Letter, Plaintiff has spent time reviewing her financial accounts and researching the impact of the Data Breach. She has also changed her email and passwords. She will be spending additional time reviewing her medical information for medical identity theft and continuing to monitor her financial accounts. Furthermore, Ms. Smith experienced actual identity theft, following the Data Breach, involving illegal and fraudulent charges appeared on her CashApp. Upon information and belief, the email account that was provided to TriHealth was also connected to CashApp. These charges were made by unknown persons attempting to pay for services she did not purchase. Ms. Smith spent additional time resolving this fraudulent activity and placed credit freezes with all of the Credit Bureaus. Ms. Smith also received notification that her email address was compromised on the Dark Web. Ms. Smith has not been notified of her data being compromised in any other data breach in the past 2 years. Upon information and belief, the fraudulent activity and identity theft she has experienced is related due to the temporal relationship and lack of other data breach notifications.

10. Plaintiff Tommie Shearer is a natural person and citizen and resident of Clermont County, Ohio. Prior to the Data Breach, Plaintiff Shearer was a patient at a TriHealth facility.

Plaintiff provided PII to TriHealth as a part of receiving medical services including date of birth, address, email address, and health insurance information. Plaintiff expected the PII and PHI to be secure and confidential and that TriHealth would implement adequate data security as part of the medical services. Plaintiff received a Notice Letter dated April 6, 2021 informing Plaintiff that the PII and PHI that had been entrusted to Defendant had been compromised in a Data Breach. As a result of receiving the Notice Letter, Plaintiff has spent time reviewing financial accounts and researching the impact of the Data Breach. Plaintiff will be spending additional time reviewing his medical information for medical identity theft and continuing to monitor his financial accounts. Furthermore, Plaintiff has received notification that Plaintiff's PII has been found on the Dark Web. Upon information and belief, Dark Web activity is connected to the TriHealth breach.

11. A copy of the letter sent to Plaintiffs and Class Members is attached as Exhibit A. ("Notice Letter").

12. Defendant TriHealth, Inc. is a domestic non-profit corporation headquartered in Cincinnati, Ohio. Service of Process is proper at OSAC, INC, 100 Third Street, Columbus, Ohio 43215.

JURISDICTION & VENUE

13. Upon information and belief, this is a local controversy where the defendant is an Ohio corporation and two-thirds (2/3) or more of the putative class members are citizens of Ohio providing exclusive jurisdiction to Ohio State Courts.

14. Venue is proper as Hamilton County is the County in which the Defendant has its principal place of business and a substantial portion of the events that form the basis of this Class Action Complaint occurred in Hamilton County, Ohio.

GENERAL FACTUAL ALLEGATIONS

THE RANSOMWARE ATTACK WAS FORESEEABLE

15. It is well known that Sensitive Information, including medical information health insurance information, dates of birth with names and addresses, is a valuable commodity and frequent target of criminal attacks.

16. The medical community is aware of numerous recent data breaches on medical facilities and their vendors.

17. In May 2019, the American Medical Collection Agency (AMCA) reported that an 8 month data breach had exposed more than 20 Million patients. This event brought into focus the risk faced when healthcare providers work with outside vendors and allow access to their systems.

18. And according to the United States Cybersecurity & Infrastructure Security Agency:

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

<https://www.cisa.gov/ransomware> (last visited Apr. 16, 2021).

19. Since these warnings, healthcare related breaches have continued to rapidly increase, and yet TriHealth failed to exercise the reasonable care in hiring, training, and supervising its employees and agents to implement necessary data security and protective measures.

**PRIVACY AND AN UNDERSTANDING THAT TRIHEALTH WOULD TAKE
ADEQUATE STEPS TO PROTECT THE PII AND PHI WAS AN IMPLICIT
TERM OF THE CARE AND TREATMENT**

20. Confidentiality is a cardinal rule of the provider-patient relationship.
21. Since 2011, TriHealth provides written Notice of Privacy Practices to all of its patients.¹
22. The Privacy Notice identifies specific reasons for disclosing a patients' PHI. This includes limited use: (1) for treatment, (2) payment, and (3) health care operations.² Additional purposes for disclosure are contained on "The Notice of Privacy Practices" page -e.g., Research, Appointment Reminders, Organ and Tissue Donation, Lawsuits, Law Enforcement.³
23. In consideration for such Privacy, the patients agree to pay for the healthcare services.⁴
24. Implied in this agreement is an understanding that TriHealth will take adequate data security measures to protect the patients PII and PHI that has been provided to TriHealth.

***DEFENDANT'S AFFIRMATIVE ACTIONS & OMISSION EXPOSED
PLAINTIFFS' AND CLASS MEMBERS' SENSITIVE INFORMATION IN A
CRIMINAL DATA BREACH***

25. As a condition of engaging in health services, Defendant required that Plaintiffs and Class Members entrust them with Sensitive Information.⁵ This Sensitive Information included social security numbers, dates of birth, address, email addresses, health insurance information, and phone numbers,
26. This Sensitive Information is subsequently shared with its vendor and agent Bricker

¹ file:///C:/Users/GBSADMIN/Downloads/physician-office-consent-2011.pdf (last visited October 1, 2021)

² *Id.*

³<https://www.trihealth.com/about-trihealth/notice-of-privacy-practices/Notice-of-Privacy-Practices---Physician-Practices.aspx> (effective Since July 1 2015)(last visited October 1, 2021)

⁴ *Id.*

⁵TriHealth Physician Partners Registration Form file:///C:/Users/GBSADMIN/Downloads/tpp-registration-form-2012.pdf_(last visited October 1, 2021)

& Eckler, LLP (“Bricker”). All the data sets and precise purpose for which the Sensitive Information was shared with Bricker is unknown and within the control of Defendants.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ Sensitive Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs’ and Class Members’ Sensitive Information from disclosure.

28. Regardless of the purpose of sharing the sensitive information with Bricker, TriHealth, individually, and/or jointly with Bricker, owed a duty to Plaintiffs to protect the data against the foreseeable criminal cyberattacks, and Defendant breached that duty by failing to incorporate adequate data security measures to keep the Sensitive Information confidential.

29. Upon information and belief, TriHealth, individually and/or jointly with Bricker, failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of its customers’ personal information in compliance with industry recognized cybersecurity framework on in compliance with FTC guidelines.

30. Because of its failure to create, maintain, and/or comply with an adequate cybersecurity program, Defendant was unable to protect Plaintiffs and Class Members Sensitive Information against obvious and readily foreseeable threats.

31. Defendant further failed to implement reasonable retention and data deletion policies to protect patients from foreseeable data breaches against Bricker.

32. As a result of Defendant’s affirmative actions and omissions, Plaintiffs’ and class members’ Sensitive Information were exposed in a targeted criminal Data Breach.

The Data Breach

33. In the Spring of 2021, Plaintiffs each received The Notice Letter from Bricker advising Plaintiffs that their Sensitive Information that was entrusted to Defendant was part of a criminal data breach. Plaintiffs were specifically informed that Bricker's computer systems were attacked and compromised in a targeted hacking and ransomware attack, in which Plaintiffs' and other patients' Sensitive Information had been accessed and stolen. The type of data specified in the letter was the patient's name, address and health-related information (the "Data Breach" and "Breach").

34. The Notice Letter further notified Plaintiffs that "Bricker implemented additional security protocols designed to enhance the security of Bricker's network, internal systems and applications." In other words, the Data Breach occurred because Bricker, Defendant's legal representative and agent, failed to implement adequate and reasonable cyber security procedures and protocols to protect Plaintiffs' Sensitive Information. Indeed, the deficiencies in Defendant's legal representative and agent's data security protocols and practices were so significant that unknown and unauthorized persons were able to access, view, remove, or download and then delete patient data.

35. Plaintiffs have no ability to confirm the types of personal information that was acquired by the third-party criminals without discovery, but upon information and belief, the personal information that was compromised in the data breach also included, at a minimum, dates of birth, email addresses, treatment information, and insurance information.

36. Plaintiffs' belief that the comprised data includes additional data categories not specially described in the Notice letter is based in part by comparing the TriHealth Notice Letter to the Adena Healthcare Notice Letter that was part of the same data breach. In the Adena Notice letter, attached as Exhibit B, Bricker included additional types of data: i.e., email addresses, phone

numbers, dates of birth, treatment information and health insurance information.

37. Moreover, both Notice Letters mention that the criminals “accessed certain Bricker internal systems at various times between January 14th, 2021 and January 31st, 2021.” It is a reasonable inference to believe that Bricker’s systems that were compromised during the same time frame contained the same types of data for Adena and TriHealth. And, notably, the TriHealth Notice letter doesn’t exclude specific data sets and but rather uses broad categories, i.e., “personal information” and “health related information” that could include dates of birth, Social Security Numbers, medical record numbers, driver’s license numbers, specific treatment information, and health insurance information, all of which are the types of data that are routinely provided by patients for healthcare services, and also are the types of information provided to law firms for HIPAA and other compliance matters.

38. Given the PII and PHI that is at issue, the targeting by criminal actors, and the reports of misuse of Plaintiff’s and class member data on the Dark Web, the risk of identity theft is real and concrete and not hypothetical.

39. Indeed, the Notice Letter acknowledges the real and concrete risk by providing information on “Identity Theft Protection” and states: “We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.” Bricker has gone as far to offer Identity Theft protection as a precaution.

40. While Bricker addresses the risk of financial Identity Fraud, the type of information at issue here also raises risk for medical identity fraud. It is well recognized that compromised health information can lead to falsified information in medical records and to fraud that can persist

for years as it “is also more difficult to detect taking twice as long as normal identity theft.”⁶ Bricker’s mitigation efforts and offers of compromise do nothing to address this risk to Plaintiffs and the Class.

The Value of the Stolen Data

41. Stolen PII and PHI are valuable commodities to identity thieves. The purpose of stealing large blocks of Sensitive Information, like in this Data Breach, is to use the data for illicit purposes or to sell the data for profit to other criminals who buy the data and misuse it.

42. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing \$16.8 billion to be stolen.⁷

43. Medical data has particular value on the black market because it often contains all of an individual’s Sensitive Information, as opposed to a single market that may be found in a more benign data breach.

44. According to a Trustware report, a healthcare data record may be valued up to \$250 a record on the black market compared to \$5.40 for the next highest value (a payment card).⁸

45. Healthcare related data is among the most sensitive and personally consequential when compromised. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery” reported Pam Dixon, executive director of World

⁶ FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusion, FBI (Apr. 8, 2014, <https://publicintelligence.net/fbi-health-care-cyber-intrusions/>).

⁷ Javelin Strategy & Research, Identity Fraud Hits All Time High With 16.7 Million US Victims in 2017. According to New Javelin Strategy & Research Study (Feb. 6, 2018), <https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin> (last visited May, 29th, 2021)

⁸ <https://www.securelink.com/blog/healthcare-data-new-prize-hackers> citing <https://trustwave.azureedge.net/media/16096/2019-trustwave-global-security-report.pdf?rnd=132056250120000000>.

Privacy Forum.⁹ A report focusing on health care breaches found that the “average total cost to resolve an identity theft related incident came to about \$20,000.”¹⁰

46. Medical information is some of the highest value data.¹¹ In fact, according to FBI’s Cyber Division, healthcare records can be sold by criminals for 50 times the price of stolen Social Security numbers or credit card numbers.¹² By one estimate, PHI can sell for as much as \$363 according to the Infosec Institute.¹³ And files containing PHI can be bought on the black market for between \$1,200 and \$1,300 each.¹⁴

47. Thus, the compromised PII and PHI of Plaintiffs and class members have a high value in both legitimate and black markets. And Plaintiffs and class members have now lost the economic value of their PII and PHI.

DEFENDANT’S CONDUCT VIOLATED HIPAA, FEDERAL TRADE COMMISSION & INDUSTRY STANDARDS ON DATA SECURITY PRACTICES

48. Defendant was and is required to maintain the security and privacy of the PII and PHI entrusted to it. Defendant, individually and collectively through its agent and legal representative Bricker, failed to properly implement basic security practices.

⁹ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News (Feb. 7 2014), <https://khn.org/news/rise-of-identity-theft/>

¹⁰ Elinor Mills, Study: Medical Identity theft is costly for victims, CNET (Mar.3, 2010) <https://www.cnet.com/tech/services-and-software/study-medical-identity-theft-is-costly-for-victims/>

¹¹ Calculating the Value of a Data Breach -What are the Most Valuable Files to a Hacker” Donnellon McCarhty Enters (July 21, 2020) <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/>

¹² See FBI supra. 1.

¹³ Data Breaches: In the Health Care Sector, Center for Internet Security, <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/>

¹⁴ Elizabeth Clarke, Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs, and Counterfeit Documents Secure Works (July 15, 2013), <https://www.secureworks.com/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-ssns-and-counterfeit-documents>

49. Defendant had numerous statutory, regulatory, and common law duties to Plaintiffs and class members to keep their PII and PHI confidential, safe, secure, and protected from unauthorized disclosure or access, including duties under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

HIPAA Standards & Violations

50. By obtaining, collecting, and using Plaintiffs’ and class members’ PII and PHI in the procurement and provision of services to Plaintiffs and class members, and ultimately deriving benefit therefrom, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs’ and class members’ sensitive information.

51. Furthermore, under Ohio law, a healthcare provider may not disclose personally identifiable, non-public information about a patient without the patient’s express written authorization.

52. Ohio Rev. Code § 3798.04 provides that a covered entity, such as a Hospital, shall not “use or disclose protected health information without any authorization that is valid under 45 C.F.R. 164.508, and if applicable, 42 C.F.R. part 2, except when the use or disclosure is required or permitted without such authorization by Subchapter C of Subtitle A of Title 45 of the Code of Federal Regulations and, if applicable, 42 C.F.R. part 2.”

53. The Data Breach resulted from a combination of insufficiencies that indicate the Defendant failed to comply with safeguards mandated by Federal and State Law and industry standards. The security failures included but are not limited to:

- A. Failing to maintain an adequate security system to prevent data loss;
- B. Failing to implement policies and procedures that limit use and disclosure of PII and PHI to its vendors to the minimum necessary;
- C. Failing to mitigate the risks of data breach and loss of data;

D. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. 164.306(a)(1);

E. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access to only those persons or software programs that have been granted access in violation of 45 C.F.R. 164.312(a)(1);

F. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R 164.308(a)(1);

G. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

H. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

I. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

J. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

FTC Guidelines & Violations

54. The Defendant also failed to comply with Federal Trade Commission (“FTC”) Guidelines.

55. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed for authorized purposes; encrypt information stored on computer networks,

understand their networks vulnerabilities; and implement policies to correct any security problems.¹⁵

56. The FTC further recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords; use industry tested methods for security; monitor for suspicious activity on the network; and verify that third party providers, such as Bricker, have implemented reasonable security measures.¹⁶

Industry Standards & Violations

57. TriHealth's failures also violated industry standards for data security practices.¹⁷

58. HHS's Office for Civil Rights ("DHHS") highlights several basic safeguards that are easily implemented to improve cybersecurity in the healthcare industry. These steps include: (1) proper encryption of PII and PHI; (2) educating and training healthcare employees and agents on how to protect PHI and PII; and (3) correcting the configuration of software and network devices.

PLAINTIFFS AND CLASS MEMBERS ARE AT AN INCREASED RISK OF IDENTITY THEFT AS A RESULT OF DEFENDANT'S ACTIONS

59. As observed in the Trend Micro analysis of the DoppelPaymer ransomware, the ransomware is not employed until the hacker has gained access to high-value information and

¹⁵ Federal Trade Commission, Protecting Personal Information: A Guide for Business, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed September 24, 2021)

¹⁶ Federal Trade Commission, Start With Security, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited September 24th, 2021)

¹⁷ HIPAA Journal, Cybersecurity Best Practices for Healthcare Organizations, <https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/> (last accessed September 24th, 2021)

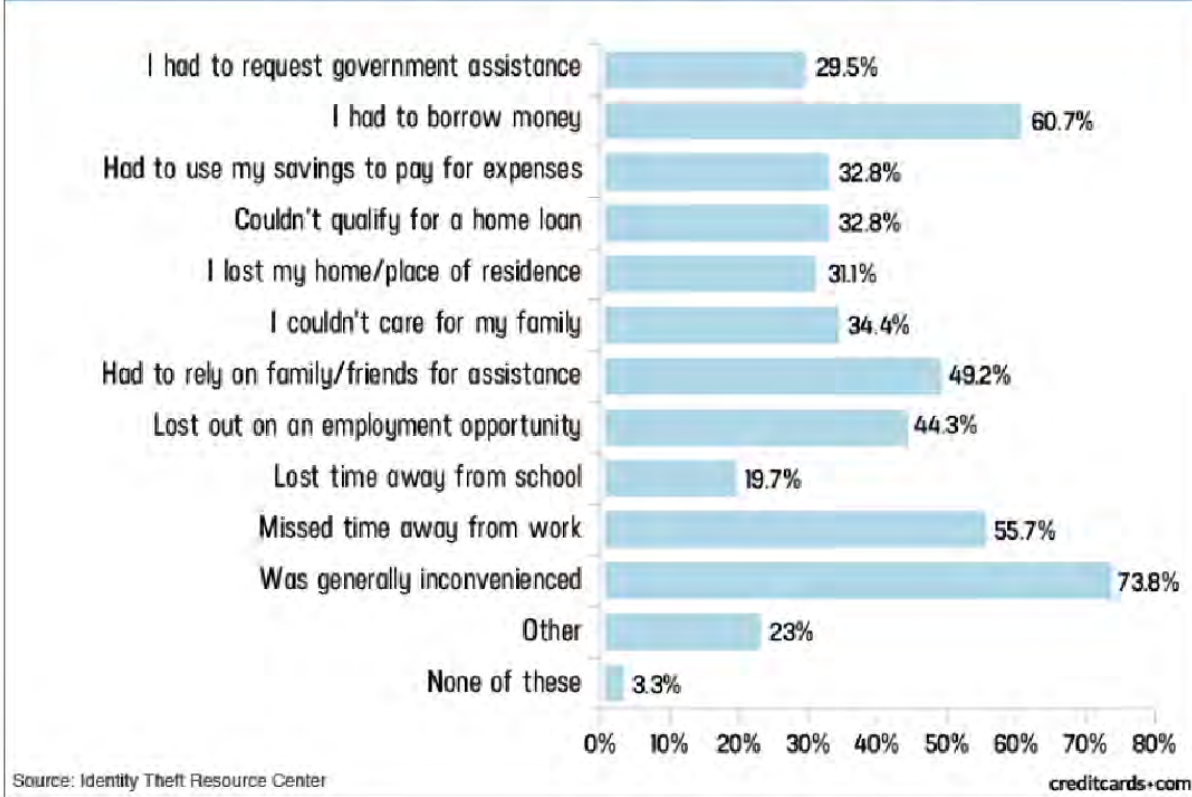
systems. Once the hackers have secretly searched the system to their satisfaction, they execute the ransomware, which encrypts what is believed to be the most sensitive or valuable files. As a result, Plaintiffs and the class members have the reasonable belief that their PII and PHI is now in the hands of hackers that will or already have misused their data or sold it to other criminals who have or will do so in the future.

60. Identity thieves use another's personal information, including dates of birth, addresses, health insurance, and health information for a variety of crimes, including credit card fraud, phone or utilities fraud, mortgage fraud, auto loans, bank/finance fraud, disability and unemployment benefits fraud, and medical identity theft.

61. In addition, identity thieves may 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.

62. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

Americans' expenses/disruptions as a result of criminal activity in their name [2016]



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Apr. 19, 2021).

63. According to the Electronic Privacy Information Center:

Identity theft is an enormous problem for consumers. The Federal Trade Commission reported 399,225 cases of identity theft in the United States in 2016. Of that number, 29% involved the use of personal data to commit tax fraud. More than 32% reported that their data was used to commit credit card fraud, up sharply from 16% in 2015. A 2015 report from the Department of Justice found that 86% of the victims of identity theft experienced the fraudulent use of existing account information, such as credit card or bank account information. The same report estimated the cost to the U.S. economy at \$15.4 billion.

64. Thus, based on the recognized statistical research, the type of data at issue, the criminal activity at issue in this case, and the report of at least one Plaintiff experiencing fraud and receiving notice of Dark Web activity, there is a strong probability that entire batches of stolen Sensitive Information have been dumped on the black market or are yet to be dumped on the black market, placing Plaintiffs and the other class members at an increased risk of fraud and identity theft for many years into the future.¹⁸

The Breach Justifies Reasonable Mitigation Efforts

65. It is well recognized that in data breaches fraudulent activity may not show up for prolonged periods of time -potentially years after PHI and PII are divulged to third party criminals. By some accounts, forty percent of consumers discovered they were victims of medical identity theft only after they received collection letters from creditors for expenses incurred in their names.¹⁹

66. Here, not only was sensitive medical information divulged but also health insurance information, dates of birth, addresses, and names. While it is unknown whether social security numbers were involved, social security numbers are not necessary for medical or financial identity theft with the PHI and PII that is known to have been disclosed in this case.

67. Despite Defendant's failure to protect Plaintiffs' and class members' PII and PHI, TriHealth has not offered Plaintiffs or class members any recourse. Bricker, its agent and legal representative, has offered the trivial and inadequate remedy of free credit monitoring or identity protection services for a short period of time that will not adequately protect them or compensate

¹⁸ <https://epic.org/privacy/data-breach/equifax/> (last visited Apr. 19, 2021).

¹⁹ The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches, Experian (Apr. 2010) <https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf>

them for their loss. For example, the Notice Letter does not even advise Plaintiffs and class members to contact their insurance companies to advise them of the breach, despite the fact that insurance information was at issue. The Notice Letter only addresses potential financial fraud but is practically useless for addressing the risk of medical identity fraud, which is also at heightened risk due to the type of information at issue in this Breach.

68. Prior to the Data Breach, Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiffs and Class Members, as current and former patients, and current and former employees, relied on Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this information.

69. In an effort to follow Bricker's advice and mitigate the risk and potential losses, Plaintiffs have spent time reviewing bank accounts and insurance information looking for suspicious activity, researching the Breach, and otherwise spending time on this Data Breach. Plaintiffs will continue to spend time each week monitoring accounts in the future and remains at risk for future identity theft (financial and medical). These efforts are reasonable in light of the current and future risk of identity theft.

70. And these efforts are in line with FTC recommendations. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (or an extended fraud alert that lasts for seven years if they learn someone has abused their information), reviewing their credit reports, contacting companies to dispute fraudulent charges on accounts, placing a credit freeze on their credit, and correcting their credit reports.²⁰

²⁰ See <https://www.identitytheft.gov/Steps> (last visited Apr. 19, 2021).

THE DATA BREACH WAS PREVENTABLE

71. Data breaches are preventable.²¹ As Lucy Thompson wrote in the Data Breach and Encryption Handbook, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”²² She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised.”²³

72. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”²⁴

PLAINTIFFS’ AND CLASS MEMBERS’ DAMAGES

73. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security, or agent’s data security systems were breached, including the significant costs that would be imposed on Plaintiffs and the Class as a result of the breach.

74. As a direct and proximate result of TriHealth’s conduct, Plaintiffs and the other class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

75. As a result of the Data Breach, Plaintiffs and the other class members must now be

²¹ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in* Data Breach and Encryption Handbook (Lucy Thompson, ed., 2012).

²² *Id.* at 17.

²³ *Id.* at 28.

²⁴ *Id.*

vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. The need for additional monitoring for identity theft and fraud will extend indefinitely into the future.

76. Plaintiffs and the other class members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Data Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiffs and the other class members suffer ascertainable losses in the form of out-of-pocket expenses and the time and costs reasonably incurred to remedy or mitigate the effects of the Breach, including:

- A. Monitoring compromised accounts for fraudulent charges;
- B. Canceling and reissuing credit and debit cards linked to the financial information in possession of the Defendant;
- C. Purchasing credit monitoring and identity theft protection;
- D. Addressing their inability to withdraw funds linked to compromised accounts;
- E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;
- G. Placing freezes and alerts with credit reporting agencies;
- H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;
- I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and

L. Closely reviewing and monitoring health insurance, medical information, financial accounts and credit reports for unauthorized activity for years to come.

77. Moreover, Plaintiffs and the other class members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the Sensitive Information, including making sure that the storage of data or documents containing Sensitive Information is not accessible by unauthorized persons and that access to such data is sufficiently protected.

78. Furthermore, Plaintiffs and the class members did not receive the value of the bargain for the medical services that were paid for, which included as part of the care and treatment an agreement to keep their medical information private and confidential.

79. And finally, as a direct and proximate result of Defendant's actions and inactions, Plaintiffs and the other class members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

80. In addition to the remedy for economic harm, Plaintiffs and the class members maintain an undeniable and continuing interest in ensuring that the PII and PHI that remains in the possession of Defendant is secure, remains secure, and is not subject to future theft.

CLASS ALLEGATIONS

81. **Class Definition:** Plaintiffs bring this action pursuant to Ohio Civ. R. 23, on behalf of a class of similarly situated individuals and entities (“the Class”), defined as follows:

All Ohio citizens whose personal, medical, or financial information was entrusted to Defendant TriHealth and exposed in the Data Breach.

Excluded from the Class are: (1) Defendant, Defendant’s subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities’ current and former officers and directors; (2) the Judge to whom this case is assigned and the Judge’s immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

82. All Class Members are readily ascertainable in that Defendant has access to addresses and other contact information for all Class Members which can be used to provide notice.

83. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals. Class Members can easily be identified through Defendant’s records, or by other means.

84. **Commonality and Predominance:** There are several questions of law and fact common to the claims of Plaintiffs and the other Class Members, which predominate over any individual issue, including:

A. Whether TriHealth adequately protected the Sensitive Information of Plaintiffs and the other Class Members;

B. Whether TriHealth engaged in the wrongful conduct alleged in this First Amended Complaint;

C. Whether TriHealth’s conduct was unlawful;

D. Whether TriHealth owed a duty to Plaintiffs and the Class Members to adequately protect their Sensitive Information and to provide timely and accurate notice of the Breach;

E. Whether TriHealth knew or should have known that Bricker's file software was vulnerable to attack;

F. Whether TriHealth adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the Sensitive Information of Plaintiffs and the other Class Members;

G. Whether TriHealth properly trained and supervised employees to protect the Sensitive Information of Plaintiffs and the other Class Members;

H. Whether TriHealth breached its duty to Plaintiffs and the other Class Members by failing to adopt, implement, and maintain reasonable policies and procedures to safeguard and protect their Sensitive Information; and

I. Whether TriHealth is liable for the damages suffered by Plaintiffs and the other Class Members as a result of the Data Breach.

85. **Typicality:** Plaintiffs' claims are typical of the claims of the other Class Members.

All claims are based on the same legal and factual issues. Plaintiffs and each of the Class Members provided Sensitive Information to Defendant and the information was accessed and disseminated for sale by unauthorized hackers. Defendant's conduct was uniform with respect to all Class Members.

86. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to the Class, and TriHealth has no defense unique to Plaintiffs.

87. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for Class Members to prosecute their claims individually. The trial and the litigation of Plaintiffs' claims are manageable.

88. Class certification, therefore, is appropriate under Ohio R. Civ. P 23(b)(3), because the common questions of law or fact predominate over any questions affecting individual Class

Members.

COUNT I

Negligence
(On behalf of Plaintiffs & the Class)

89. Plaintiffs incorporate by reference all other allegations in the complaint as if fully set forth here.

90. TriHealth knew, or should have known, of the risks inherent in collecting and storing and retaining without medical purpose the Sensitive Information of Plaintiffs and the other Class Members. TriHealth knew or should have known of the importance of adequate security. TriHealth was well aware of numerous, well-publicized data breaches that exposed the Sensitive Information of individuals. TriHealth was also aware from the FBI's publications of the risk presented by groups like the DoppelPaymer hackers.

91. TriHealth had a common law duty to prevent foreseeable harm to those who entrusted their personal, medical, and financial information to TriHealth. This duty existed because Plaintiffs and the other Class Members were foreseeable and probable victims of the failure of TriHealth or its agent to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and the other Class Members' personal, medical, and financial information would not be accessible by unauthorized persons.

92. TriHealth had a special relationship with the Plaintiffs and the other Class Members. TriHealth was entrusted with Plaintiffs' and the other Class Members' Sensitive Information, and TriHealth was in a position to protect this Sensitive Information from unauthorized access and activity. TriHealth's duties also arose under section 5 of the Federal Trade Commission Act ("FTC 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 individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of TriHealth.

93. TriHealth had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class Members' Sensitive Information in its possession so that the Sensitive Information would not come within the possession, access, or control of unauthorized persons.

94. More specifically, the duties of TriHealth included, among other things, the duty to:

A. Adopt, implement, and maintain policies, procedures, and security measures for protecting Plaintiffs' and the other Class Members' Sensitive Information, including policies, procedures, and security measures;

B. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of Plaintiffs' and the other Class Members' Sensitive Information with entities that failed to adopt, implement, and maintain policies, procedures, and security measures;

C. Adopt, implement, and maintain reasonable policies and procedures to ensure that Plaintiffs' and the other Class Members' Sensitive Information is disclosed only with authorized persons who have adopted, implemented, and maintained policies, procedures, and security measures;

D. Properly train its employees to protect documents containing Plaintiffs' and the other Class Members' Sensitive Information; and

E. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly repel breaches to the security of its systems.

95. TriHealth breached the foregoing duties and failed to exercise reasonable care in the ways described above in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and the other Class Members' Sensitive Information in its possession, custody, and care.

96. As a direct and proximate result of the conduct of TriHealth, Plaintiffs and the other Class Members have suffered and will continue to suffer non-economic damages including, but

not limited to, anxiety, emotional distress, and loss of privacy. Plaintiffs and the Class will sustain economic and non-economic damages into the future.

COUNT II

Negligent Entrustment (*On Behalf of Plaintiffs and the Class*)

97. Plaintiffs incorporate by reference all other allegations in the complaint as if fully set forth here.

98. TriHealth owed a duty to Plaintiffs and the Class to adequately safeguard the Sensitive Information that it required Plaintiffs and the Class Members to provide. Part and parcel with this duty was the duty to only entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

99. TriHealth breached this duty by entrusting Bricker with the Sensitive Information of its patients when, as described throughout the Complaint, it knew or should have known that Bricker and Bricker's legacy software was incompetent at preventing such unauthorized disclosure.

100. TriHealth further breached this duty by entrusting Bricker with the Sensitive Information of Plaintiffs and the Class Members when it failed to require Bricker to implement a deletion policy where information that was not needed or no longer needed for patient medical care, patient billing, or health care operations related to Plaintiffs or the Class.

101. As a direct and proximate result of Defendant's failure to exercise reasonable care in whom it entrusted the Class Members Sensitive Information to, the Sensitive Information of the Class Members was accessed by ill-intentioned criminals who could and will use the information to commit identity theft or financial fraud. Plaintiffs and the Class face the imminent, certainly

impending, and substantially heightened risk of identity theft, fraud, and further misuse of their Sensitive Information.

102. As a direct and proximate result of TriHealth's conduct, Plaintiffs and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiffs and the Class have suffered emotional distress as a result of the Breach and have lost time and/or money as a result of past and continued efforts to protect their Sensitive Information and prevent the unauthorized use of their Sensitive Information. Plaintiffs and the Class will sustain economic and non-economic damages into the future.

COUNT III

Breach of Implied Contract *(On behalf of the Plaintiffs and the Class)*

103. Plaintiffs incorporate by reference all other allegations in the Complaint as if fully set forth here.

104. Plaintiffs and the Class Members entered into implied contracts with TriHealth under which TriHealth agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

105. Plaintiffs and the Class were required to and delivered their Sensitive Information to TriHealth as part of the process of obtaining services provided by TriHealth. Plaintiffs and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

106. TriHealth accepted possession of Plaintiffs' and Class Members' Sensitive Information for the purpose of providing services or Plaintiffs and Class Members.

107. In accepting such information and payment for services, Plaintiffs and the other

Class Members entered into an implied contract with TriHealth whereby TriHealth became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Sensitive Information.

108. In delivering their Sensitive Information to TriHealth and paying for healthcare services, Plaintiffs and Class Members intended and understood that TriHealth would adequately safeguard the data as part of that service.

109. In their written policies and registration form, TriHealth expressly and impliedly promised to Plaintiffs and Class Members that it would only disclose protected information and other Sensitive Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

110. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

111. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII or PHI also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption from Bricker; and (6) other steps to protect against foreseeable data breaches.

112. Plaintiffs and the Class Members would not have entrusted their Sensitive Information to TriHealth in the absence of such an implied contract.

113. Had TriHealth disclosed to Plaintiffs and the Class that it would entrust such data

to incompetent third-party agents that did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Sensitive Information to TriHealth.

114. TriHealth recognized that Plaintiffs' and Class Member's personal data is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

115. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with TriHealth.

116. TriHealth breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their data as described herein.

117. As a direct and proximate result of TriHealth's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV

Unjust Enrichment *(On behalf of the Plaintiffs and the Class)*

118. Plaintiffs incorporate by reference all other allegations in the complaint as if fully set forth herein.

119. TriHealth failed to provide reasonable security, safeguards, and protections to the Sensitive Information of Plaintiffs and Class Members, instead entrusting such data to Bricker through Bricker's outdated and vulnerable software, and as a result Plaintiffs and the Class overpaid TriHealth as part of the services they purchased.

120. TriHealth failed to disclose to Plaintiffs and Class Members that Bricker's practices and software and systems (which TriHealth chose to utilize) were inadequate to safeguard

Plaintiffs' and the Class Members' Sensitive Information against theft.

121. Under principles of equity and good conscience, TriHealth should not be permitted to retain the money belonging to Plaintiffs and Class Members because TriHealth failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Sensitive Information. Accordingly, Plaintiffs and the other Class Members paid for services that they did not receive.

122. TriHealth wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

123. TriHealth's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

124. As a result of TriHealth's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by TriHealth, plus attorneys' fees, costs, and interest thereon.

COUNT V

Vicarious Liability (On behalf of the Plaintiffs and the Class)

125. Plaintiffs incorporate the previous paragraphs of this Complaint as if fully restated here.

126. At all relevant times, Bricker was the agent and/or independent contractor of TriHealth.

127. Bricker was negligent by failing to take adequate steps to protect the PII and PHI that was provided by TriHealth. Bricker's negligence, independently or in combination with TriHealth's negligence, allowed the third-party criminals to access Plaintiffs' and Class Members' PII and PHI.

128. As a direct and proximate result of the negligence of its agent, and/or independent contractor, TriHealth is vicariously liable for the injuries and damages described above and Plaintiffs and the Class are entitled to compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs individually, and on behalf of all others similarly situated, respectfully requests that judgment be entered in their favor and against TriHealth as follows:

- A. That the Court find that this action satisfies the prerequisites for maintenance as a class action and certifies the Class defined herein;
- B. That the Court appoint Plaintiffs as representatives of the Class;
- C. That the Court appoint Plaintiffs' counsel as counsel for the Class;
- D. That the Court enter judgment in favor of Plaintiffs and the Class against TriHealth;
- E. That the Court award Plaintiffs and the other Class members actual damages and all other forms of available relief, as applicable;
- F. That the Court award Plaintiffs and the Class attorney's fees and costs, including interest thereon as allowed or required by law;
- G. That the Court enter an injunction requiring Defendant to adopt, implement, and maintain adequate security measures to protect its customers' personal and financial information; and
- H. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs, individually and on behalf of all others similarly situated, hereby demand a trial by jury on all claims so triable.

Respectfully submitted,

/s/ Joseph M. Lyon

Joseph Lyon (0076050)
THE LYON FIRM, LLC
2754 Erie Ave
Cincinnati, Ohio 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

Jeffrey S. Goldenberg (0063771)
Todd B. Naylor (0068388)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
Email: jgoldenberg@gs-legal.com
tnaylor@gs-legal.com

Marc E. Dann (0039425)
Brian D. Flick (0081605)
Michael Smith (0097147)
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Counsel for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I hereby certify that on this 1st day of October, 2021, I served a copy of the foregoing *First Amended Complaint* upon the following parties via electronic means:

Jennifer O. Mitchell at jennifer.mitchell@dinsmore.com
Matthew Arend at matthew.arend@dinsmore.com
Dinsmore & Shohl LLP
1900 Chemed Center
255 East Fifth Street
Cincinnati, OH 45202

Counsel for Defendant TriHealth

/s/ Joseph M. Lyon
Joseph Lyon (0076050)

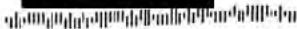
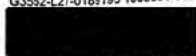
EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 6, 2021

G3552-L27-0185195 T00595 P012 *****AUTO**5-DIGIT 45176



Re: Notice of Data Security Incident

Dear [Redacted]

We are writing to you because your health care provider, TriHealth, Inc. ("TriHealth") hired our law firm, Bricker & Eckler LLP ("Bricker"), to perform legal work on its behalf. We have been counsel for TriHealth for several years. Regrettably, we have recently learned of criminal conduct that resulted in a data security incident at Bricker that involves your personal information. While, we have found no evidence that your personal information was misused, we take this matter and the security of your personal information very seriously.

Bricker was recently the target of a ransomware attack, which is a type of cyber-attack. Bricker services companies and organizations across a variety of industries, and in the course of its work on behalf of clients is at times provided access to personal information as a part of the client engagement. Bricker receives and utilizes this data solely in its representation of and to provide legal counsel to its clients, including TriHealth.

This notice explains the incident, steps Bricker has taken in response, and additional information on steps you may take to help protect your information.

What Happened?

On January 31, 2021, Bricker learned that it was the target of a criminal ransomware attack. Upon learning of the incident, Bricker immediately took measures to contain the incident, launched an investigation, and third-party cybersecurity forensic experts were engaged to assist. Bricker notified TriHealth of the incident on February 5, 2021 and, after a thorough and exhaustive forensic investigation, informed TriHealth on March 3, 2021 that, in fact, personal information for a substantial number of TriHealth patients and employees was involved. Bricker also notified federal law enforcement.

The investigation determined that an unauthorized party gained access to certain Bricker internal systems at various times between approximately January 14, 2021 and January 31, 2021. Findings from the investigation indicate that the party obtained spreadsheets and other documents containing personal information from certain Bricker systems during this period. Bricker was able to retrieve the data which included your personal information from the unauthorized party and has taken steps to confirm that the unauthorized party deleted the data related to TriHealth. At this time, Bricker has received no indication that this data was further copied or retained by the unauthorized party. Bricker conducted a thorough review of the data to identify individuals whose personal information may have been involved.

018695



G3552-L27

What Information Was Involved?

The review determined that the data involved contained some of your personal information, including your name, address, and health-related information.

What We Are Doing

To help prevent a similar type of incident from occurring in the future, Bricker implemented additional security protocols designed to enhance the security of Bricker's network, internal systems and applications. Bricker will also continue to evaluate additional steps that may be taken to further increase Bricker's defenses going forward. In addition, Bricker is continuing to support federal law enforcement's investigation and has recovered all the data that was stolen from its systems.

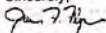
What You Can Do

At this time, Bricker has no indication that your personal information has been misused, but Bricker wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. As a precaution, Bricker is offering you a complimentary one-year membership in Experian® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score. For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For More Information

Again, the security of your personal information is important to Bricker and to TriHealth. Bricker sincerely regrets that this incident occurred. We apologize for the stress and worry this situation has caused you and are doing everything we can to rectify the situation. Please remain vigilant reviewing account statements and credit reports. For more information, or if you have any questions or need additional information, please call (833) 796-8641, Monday through Friday, between 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern Time.

Sincerely,



James Flynn
Managing Partner
Bricker & Eckler LLP

Experian Enrollment Information

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: July 31, 2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: Z5ZR5XNT

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 796-8641 by July 31, 2021. Be prepared to provide engagement number DB26427 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-Month EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance¹:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 796-8641. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one-year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies — Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-8085318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-7430023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1800-697-1220, <http://www.dps.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

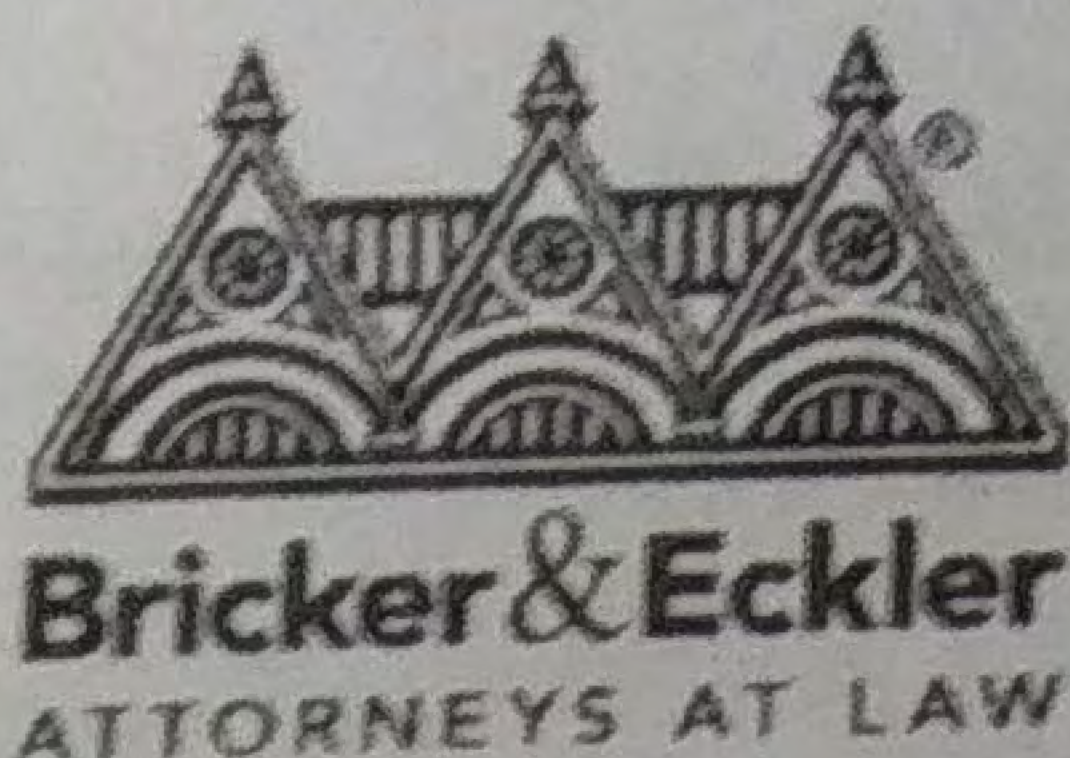
For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.



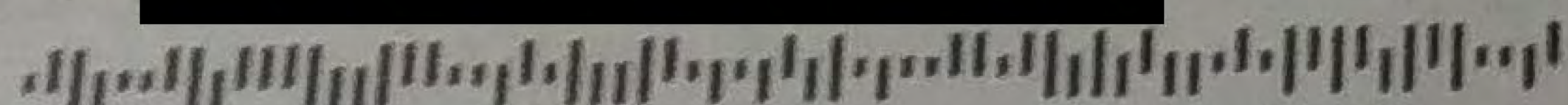
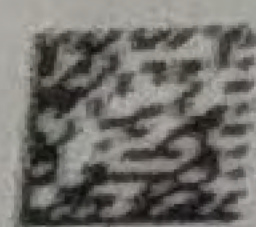
EXHIBIT B



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 6, 2021

G3552-L14-0135851 T00428 P010 *****AUTO**5-DIGIT 45053



Re: Notice of Data Security Incident

Dear [REDACTED]

Bricker & Eckler LLP ("Bricker"), a full-service law firm with offices throughout Ohio and clients across the country, was recently the target of a ransomware attack. Bricker services companies and organizations across a variety of industries, and in the course of its work on behalf of clients is at times provided access to personal information as a part of the client engagement. Bricker receives and utilizes this data solely in its representation of and to provide legal counsel to its clients.

Bricker is writing to inform you that the incident may have involved some of your personal information. Bricker was in possession of that information due to its work on behalf of ADENA HEALTH SYSTEM. This notice explains the incident, steps Bricker has taken in response, and additional information on steps you may take to help protect your information.

What Happened?

On January 31, 2021, Bricker learned that it was the target of a ransomware attack. Upon learning of the incident, Bricker immediately took measures to contain the incident, launched an investigation, and third-party cybersecurity forensic experts were engaged to assist. Bricker also notified federal law enforcement.

The investigation determined that an unauthorized party gained access to certain Bricker internal systems at various times between approximately January 14, 2021 and January 31, 2021. Findings from the investigation indicate that the party obtained some data from certain Bricker systems during this period. Bricker was able retrieve the data involved from the unauthorized party and has taken steps to delete the data. At this time, Bricker has no reason to believe this data was further copied or retained by the unauthorized party. Bricker conducted a thorough review of the data to identify individuals whose personal information may have been involved. On or around March 12, 2021, Bricker substantially completed its review of the data and began formally notifying clients of any client-related personal information included in these files.

What Information Was Involved?

The review determined that the data involved contained some of your personal information, which may have included your name, address, email address, phone number, date of birth, and information related to care received at Adena Health System, such as treatment and/or health insurance information

What We Are Doing

To help prevent a similar type of incident from occurring in the future, Bricker implemented additional security protocols designed to enhance the security of Bricker's network, internal systems and applications. Bricker will also continue to evaluate additional steps that may be taken to further increase Bricker's defenses going forward. In addition, Bricker is continuing to support federal law enforcement's investigation.

What You Can Do

At this time, there is no evidence that your personal information has been misused, but Bricker wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. As a precaution, Bricker is offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

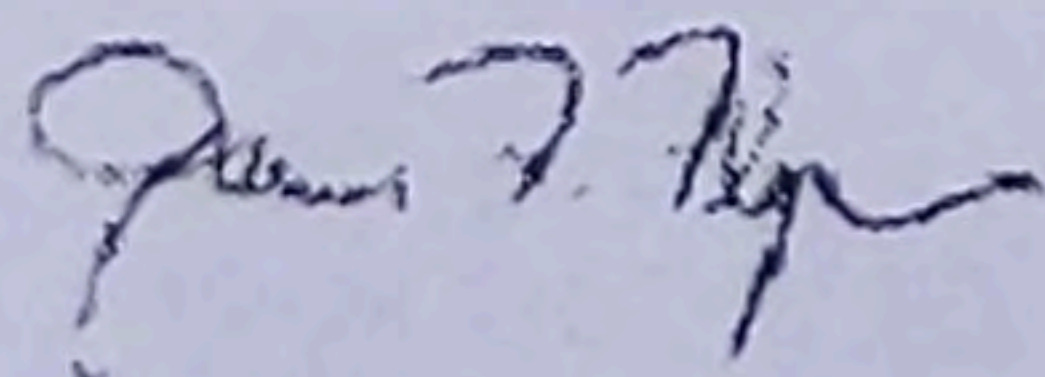
- Ensure that you enroll by: July 31, 2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: Y2QPZVKP6

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (833) 796-8641 by July 31, 2021. Be prepared to provide engagement number DB26427 as proof of eligibility for the identity restoration services by Experian.

For More Information

The security of your personal information is important to Bricker and Bricker sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call (833) 796-8641, Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern.

Sincerely,



James Flynn
Managing Partner
Bricker & Eckler LLP

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 796-8641. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.