

1 MEYER WILSON CO., LPA  
2 Matthew R. Wilson, Esq. (SBN 290473)  
3 [mwilson@meyerwilson.com](mailto:mwilson@meyerwilson.com)  
4 Michael J. Boyle, Jr. (SBN 258560)  
5 [mboyle@meyerwilson.com](mailto:mboyle@meyerwilson.com)  
6 305 W. Nationwide Blvd  
7 Columbus, OH 43215  
8 PH: 614-224-6000  
9 Fax: 614-224-6066

E-FILED  
1/20/2022 8:00 AM  
Superior Court of California  
County of Fresno  
By: E. Meyer, Deputy

*Attorneys for Plaintiffs and the Proposed Class*

**IN THE SUPERIOR COURT  
FOR THE COUNTY OF FRESNO**

Case No. **22CECG00285**

10 NAREK AVETISYAN, on behalf of  
11 himself and all others similarly situated,

**Class Action Complaint**

*Plaintiff,*

v.

14 UNITED HEALTH CENTERS OF THE  
15 SAN JOAQUIN VALLEY.

*Defendant.*

**INTRODUCTION**

18 1. Defendant United Health Centers of the San Joaquin Valley (“UHC”) is a healthcare  
19 provider that creates and stores intimate personal health information (“PHI”) and personally  
20 identifying information (“PII”) (collectively, the “Sensitive Information”) about its patients—  
21 including, for example, their names, medical diagnoses, drug prescriptions, lab test results, and social  
22 security numbers. But as a result of UHC’s negligence, a third-party accessed that data beginning on  
23 August 28, 2021 as part of a “ransomware” attack. UHC knew as of at least September 22, 2021 that  
24 information was compromised—including extremely sensitive information such as Social Security  
25 numbers and diagnosis information—but sat on this information entirely for almost two months,  
26 leaving their current and former patients helpless to protect themselves from criminals who may have  
27 bought or sold their medical and financial information.  
28

1           2.       Plaintiffs are former patients of UHC whose Sensitive Information was exposed in the  
2 breach. They seek damages and equitable relief on behalf of themselves and all others similarly  
3 situated.

4                                       **PARTIES**

5           3.       Plaintiff Narek Avetisyan is a resident of Clovis, California.

6           4.       Defendant UHC is a California corporation engaged in the business of providing health  
7 care services. Its principal place of business is located at 3875 West Beechwood Avenue, Fresno,  
8 California 93722.

9                                       **JURISDICTION & VENUE**

10          5.       Plaintiffs bring a private cause of action under the Confidentiality of Medical  
11 Information Act, CIV. CODE § 56, *et seq.*; the Consumer Records Act, CIV. CODE § 1798.80, *et seq.*;  
12 the Unfair Competition Law, BUS. & PROF. CODE § 17200, *et seq.*; and the common law of  
13 California.

14          6.       UHC is a California corporation subject to this Court’s general jurisdiction.

15          7.       Venue is proper in the Fresno County Superior Court because the Defendant’s  
16 principal place of business is located therein.

17          8.       Because UHC is a medical provider with its headquarters in Fresno, California and  
18 medical care locations in Fresno, Tulare, and Kings Counties, California, on information and belief,  
19 at least two-thirds of the proposed class members reside in California.

20  
21  
22  
23  
24  
25  
26  
27  
28

1 **FACTUAL ALLEGATIONS**

2 **A. UHC Collects and Maintains Personal and Medical Information**

3 10. UHC is a medical services conglomerate that operates 25 Health Centers in Fresno,  
4 Tulare, and Kings Counties, California.<sup>1</sup> UHC’s Health Centers provide a wide variety of medical  
5 services, including general and family medicine, pediatrics, general dentistry, clinical laboratory, X-  
6 ray, dermatology, telemedicine, integrated behavioral health, chiropractic care, optometry, and  
7 preventative medicine programs.<sup>2</sup>

8 11. As a healthcare provider, UHC creates, maintains, preserves, and stores data  
9 concerning its patients. This Sensitive Information includes patients’ names, addresses, phone  
10 numbers, Social Security numbers, driver’s license numbers, diagnoses, treatment and prescription  
11 information, provider names, patient IDs, Medicare/Medicaid numbers, lab test results, health  
12 insurance information, and treatment cost information.

13 12. The information contained in that data is “sensitive” and “personal” to its patients. Any  
14 reasonable person would find that unauthorized accessed to such personal and confidential medical  
15 information was highly offensive. UHC thus knew, or should have known, that its patients expected  
16 UHC to keep their Sensitive Information secure from intrusions by third parties.

17 13. It was highly foreseeable that bad actors would attempt to access UHC’s data.  
18 According to one scholar, “the healthcare industry has faced the highest number of [data] breaches  
19 among all industries.”<sup>3</sup> Indeed, “hackers are likely to be drawn to databases containing information  
20 which has a high value on secondary black markets,” such as “intimate and health-related data.”<sup>4</sup>

21  
22  
23 <sup>1</sup> <https://unitedhealthcenters.org/findahealthcenter> (last accessed January 14, 2022)

24 <sup>2</sup> <https://unitedhealthcenters.org/aboutus/whatwedo> (last accessed January 14, 2022).

25  
26 <sup>3</sup> Adil Hussain Seh, et. al, *Healthcare Data Breaches: Insights and Implications*, 8 HEALTHCARE 133,  
27 2 (2020), <https://www.mdpi.com/2227-9032/8/2/133/htm>

28 <sup>4</sup> Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55.

1 “Therefore, relevant and rational firms should engage in greater security investment and reduced  
2 collection—all steps to limit the prospects of a potential breach and subsequent notification.”<sup>5</sup>

3 14. For healthcare providers, data breaches entail a particularly severe, foreseeable risk of  
4 harm. According to the American Medical Association, “cyberattacks not only threaten the privacy  
5 and security of patients’ health and financial information, but also patient access to care.”<sup>6</sup> And the  
6 risk of identity theft carries serious implications for data breach victims: “an increased risk of identity  
7 theft is akin to the risk of contracting a chronic disease.

8 15. The risk of a data breach is ongoing. Data-breach notification letters often explicitly  
9 inform people that there is a risk of identity theft. Credit-monitoring services are generally offered for  
10 one or two years, signaling to victims an increased risk of theft for that time period.

11 16. When a person has a reasonable belief that her credit identity is in jeopardy, she is  
12 rightly afraid that her creditworthiness is out of her hands. The exposure to the risk of identity theft  
13 can be anxiety-inducing because identity theft can have catastrophic effects on an individual's life and  
14 because it is difficult to resolve. The passage of time may not dissipate that fear because identity theft  
15 can happen at any time. A person's financial and employment opportunities can be destroyed by  
16 identity theft, and time and money are essential to addressing it. In all of these ways, identity theft is  
17 the digital equivalent to contracting a chronic disease.”<sup>7</sup>

## 18 **B. The Data Breach**

19 17. On August 28, 2021, UHC was attacked by what it characterizes as “an encryption  
20  
21

---

22  
23 <sup>5</sup> *Id.* at 855.

24 <sup>6</sup> Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.  
25 ASS’N (Oct. 4, 2019), [https://www.ama-assn.org/practice-management/sustainability/cybersecurity-  
26 ransomware-attacks-shut-down-clinics-hospitals](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals).

27 <sup>7</sup> Daniel J. Solove & Danielle K. Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX.  
28 L. REV. 737, 762 (2018) (footnotes omitted).

1 event.”<sup>8</sup> On information and belief, based on public reporting in the cybersecurity community, the  
2 “encryption event” was a ransomware attack undertaken by the Vice Society cyber-gang.<sup>9</sup>

3 18. The federal Cybersecurity and Infrastructure Security Agency defines a ransomware as  
4 “a form of malware designed to encrypt files on a device, rendering any files and the systems that rely  
5 on them unusable. Malicious actors then demand ransom in exchange for decryption.”<sup>10</sup>

6 19. Ransomware attacks on healthcare providers and agencies are very common. A survey  
7 of health care providers reported that 34% of them experienced ransomware attacks in 2020.<sup>11</sup>  
8 Moreover, 2021 saw a 45% uptick in ransomware attacks against health care providers.<sup>12</sup>

9 20. Notwithstanding the known threat to health care privacy from ransomware attacks,  
10 UHC did not confirm that a breach occurred in its systems until almost a month later, on September  
11 22., 2021. Moreover, this confirmation did not come as a result of any efforts by UHC, but as a result  
12 of the PHI of UHC patients being posted to certain websites colloquially known as “the Dark Web.”<sup>13</sup>

13 21. UHC said nothing to the public or to its patients until November 19, 2021, almost three  
14 months after the incident and two months after PHI was posted on the Dark Web.<sup>14</sup> The notice of the  
15

16 \_\_\_\_\_  
17  
18 <sup>8</sup> <https://unitedhealthcenters.org/incident> (last accessed January 17, 2022).

19 <sup>9</sup> <https://cybersecuritylog.com/united-health-centers-of-san-joaquin-valley-hit-by-vice-society-ransomware> (last accessed January 17, 2022).

20 <sup>10</sup> <https://www.cisa.gov/stopransomware> (last accessed January 14, 2022).

21  
22 <sup>11</sup> “The State of Ransomware in Healthcare in 2021,” at pg. 3 (available at  
23 <https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-healthcare-2021-wp.pdf>) (last accessed January 17, 2022).

24 <sup>12</sup> <https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals> (last accessed  
25 January 17, 2022).

26 <sup>13</sup> <https://cybersecuritylog.com/united-health-centers-of-san-joaquin-valley-hit-by-vice-society-ransomware> (last accessed January 17, 2022).

27  
28 <sup>14</sup> <https://unitedhealthcenters.org/incident> (last accessed January 17, 2022).

1 incident offered no specific assistance or aid to affected patients, nor did it identify the specific  
2 patients who were impacted by the breach.

3 22. As a result of the unauthorized access to their Sensitive Information, Plaintiffs and class  
4 members suffered injury and damages, including: an increased risk of identity theft or identity fraud;  
5 improper disclosure of their medical information; the time and expense necessary to mitigate the  
6 heightened risk of identity theft or fraud; and extreme emotional distress and anxiety as a result of the  
7 heightened risk of identity theft or fraud, as well as the fact that their personal and medical information  
8 was accessed by a third-party.

9 23. Plaintiff and class members suffered (and continue to suffer) additional damages based  
10 on the opportunity cost and time Plaintiff and class members are forced to expend in the future to  
11 monitor their personal information and accounts as a result of the breach.

12 24. Those damages were increased by the unreasonable delay between when UHC learned  
13 of the breach and when it informed Plaintiffs and the Class of the breach. If UHC had provided  
14 Plaintiffs and the Class with notice in a reasonable time, they would have been able to take appropriate  
15 protective measures sooner, which would have prevented additional harm.

16 25. The data breach was caused and enabled by UHC's violation of its common law and  
17 statutory obligations to implement and maintain the kinds of security measures appropriate for  
18 protecting sensitive medical and personal information from unauthorized access, acquisition,  
19 destruction, use, and modification.

### 20 **C. Plaintiff Narek Avetisyan's Experience**

21 26. Plaintiff Narek Avetisyan received medical services on several occasions from 2016 to  
22 2019.

23 27. UHC made digital records of Avetisyan's personal and medical information.

24 28. Plaintiff Avetisyan's Sensitive Information was exposed in the data breach.

25 29. As part of his general cybersecurity practices, Plaintiff Avetisyan maintains an  
26 "Internet and Dark Web Monitoring" service offered by the American Automobile Association.

27 30. On December 8, 2021, Plaintiff Avetisyan's monitoring service notified him that his  
28 name, Social Security Number, and Date of Birth was detected on the Dark Web. The monitoring

1 report stated that the information was exposed as a result of the UHC data breach. A copy of Plaintiff  
2 Avetisyan's monitoring report is attached to this Complaint as Exhibit 1.

3 31. Plaintiff Avetisyan's monitoring service does not cover medical information in its  
4 review of the Dark Web. As a result, it is highly likely that Plaintiff Avetisyan's diagnosis and  
5 treatment information was exposed alongside his name, date of birth, and Social Security number.

6 32. Plaintiff Avetisyan has received no communication from UHC regarding the breach.  
7 Plaintiff did, however, contact the provided toll-free number provided by UHC. When Plaintiff  
8 Avetisyan contacted the toll-free number, an automated message played and provided little  
9 information about the breach.

10 33. Plaintiff Avetisyan has suffered from stress and anxiety as a result of his personal and  
11 medical information being exposed to the public, as well as the increased risk of identity theft.

12 34. Plaintiff Avetisyan was required to spend several hours investigating the data breach, a  
13 task he expects will continue to take up his time in the future.

14 35. The data breach impaired the value of Plaintiff Avetisyan's personal information.

15 36. If Plaintiff Avetisyan had been notified in a timely manner, he would have been able to  
16 take protective measures sooner, which would have limited his injuries.

17 **D. Data Breaches Lead to Identity Theft and Cognizable Injuries.**

18 37. The personal, health, and financial information of Plaintiffs and the Class, is valuable  
19 and has been commoditized in recent years.

20 38. Identity theft occurs when someone uses another's personal and financial information  
21 such as that person's name, account number, Social Security number, driver's license number, date of  
22 birth, and/or other information, without permission, to commit fraud or other crimes.

23 39. According to experts, one out of four data breach notification recipients becomes a  
24 victim of identity fraud.<sup>15</sup>

---

25  
26  
27 <sup>15</sup> *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*,  
28 ThreatPost.com (last visited, Feb. 21, 2013), <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/>

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

5           41. Once Sensitive Information is sold, it is often used to gain access to various areas of the  
6 victim’s digital life, including bank accounts, social media, credit card, and tax details. This can lead  
7 to additional Sensitive Information being harvested from the victim, as well as Sensitive Information  
8 from family, friends, and colleagues of the original victim.

9           42. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet Crime  
10 Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year,  
11 resulting in more than \$3.5 billion in losses to individuals and business victims.

12           43. Further, according to the same report, “rapid reporting can help law enforcement stop  
13 fraudulent transactions before a victim loses the money for good.” Defendant did not rapidly report to  
14 Plaintiff and the Class that their Sensitive Information had been stolen.

15           44. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in  
16 person or online, and/or experience financial losses resulting from fraudulently opened accounts or  
17 misuse of existing accounts.

18           45. Victims of identity theft often suffer indirect financial costs as well, including the costs  
19 incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in  
20 obtaining or retaining credit.

21           46. In addition to out-of-pocket expenses that can exceed thousands of dollars for the  
22 victim of new account identity theft, and the emotional toll identity theft can take, some victims have  
23 to spend a considerable time repairing the damage caused by the theft of their Sensitive Information.  
24 Victims of new account identity theft will likely have to spend time correcting fraudulent information  
25 in their credit reports and continuously monitor their reports for future inaccuracies, close existing  
26 bank/credit accounts, open new ones, and dispute charges with creditors.

27           47. Making victims’ response more difficult is the fact that data thieves may wait years  
28 before attempting to use the stolen Sensitive Information. To protect themselves, Plaintiff and the



1 Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

2 48. As a direct and proximate result of Defendant’s wrongful actions and omissions here,  
3 Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic  
4 damages, and other actual injury and harm, including, *inter alia*: (i) from the untimely and inadequate  
5 notification of the data breach, (ii) the resulting immediate and continuing risk of future ascertainable  
6 losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost  
7 time they must spend to monitor their financial accounts and other accounts—for which they are  
8 entitled to compensation; and (iv) out-of-pocket expenses for securing identity theft protection and  
9 other similar necessary services.

10 **E. Medical Data Breaches Themselves *Are* Privacy Injuries**

11 49. When it comes a breach of PHI, the injury and the harm *has already occurred*. No  
12 further disclosure is necessary. As Justice Brandeis once observed, invasions of privacy are  
13 themselves concrete injuries and, indeed, can subject victims “to mental pain and distress, far greater  
14 than could be inflicted by mere bodily injury.”<sup>16</sup>

15 50. Medical data breaches acutely implicate the right to privacy, as “[p]atients are highly  
16 sensitive to disclosure of their health information,” particularly because PHI “often involves intimate  
17 and personal facts, with a heavy emotional overlay.”<sup>17</sup>

18 51. Unsurprisingly, then, empirical evidence demonstrates that “[w]hen asked, the  
19 overwhelming majority of American patients express concern about the privacy of their medical  
20 records.”<sup>18</sup>

21 52. Plaintiff and the Class had a reasonable expectation of privacy in their PHI.  
22  
23

---

24 <sup>16</sup> Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

25 <sup>17</sup> Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33  
26 RUTGERS L.J. 617, 621 (2002).

27 <sup>18</sup> Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health  
28 Record Systems*, 24 BERKLEY TECH. L.J. 1523, 1557 (2009).

1 53. The disclosure of PHI is highly offensive to a reasonable person.

2 54. As a direct and proximate result of UHC's acts and omissions, Plaintiff and the Class  
3 suffered harm, an invasion of privacy, when their PHI was viewed by an unauthorized third-party.

4 **CLASS ACTION ALLEGATIONS**

5 55. Under CAL. CODE CIV. P. § 382, Plaintiff seeks certification of a class defined as  
6 follows:

7 Any person whose Sensitive Information was exposed to a third-  
8 party in the breach of Defendant's computer network that occurred  
9 on or after August 28, 2021.

10 56. Excluded from the Class are Defendant's employees, officers, directors, legal  
11 representatives, successors and wholly or partly owned subsidiaries or affiliated companies; class  
12 counsel and their employees; and the judicial officers and their immediate family members and  
13 associated court staff assigned to this case.

14 **A. The Class is ascertainable.**

15 57. Through the use of data mining, UHC is capable of producing a list of patients who  
16 were affected by the breach. Those records identify the Class Members.

17 **B. The Class is sufficiently numerous.**

18 58. UHC has not disclosed the number of individuals affected by the breach. However,  
19 public reporting in the cybersecurity community have described records found on the Dark Web  
20 consisting of a patient roster containing at least 5,000 entries.<sup>19</sup> Thus, the number of affected  
21 individuals is, at a minimum, in the thousands.

22 59. As a result, the proposed Class is so numerous that individual litigation would be  
23 impracticable.

24

25

26

27

---

<sup>19</sup> <https://www.databreaches.net/united-health-centers-of-san-joaquin-valley-remains-publicly-silent-after-ransomware-attack/> (last accessed January 17, 2022).

28

1 **C. The Class constitutes a well-defined community of interest.**

2 60. The proposed class constitutes a well-defined community of interest, as demonstrated  
3 by the predominance of common issues, the typicality of Plaintiff's claims to those of the Class, and  
4 the adequacy of Plaintiff and his counsel as class representatives.

5 61. *Predominance.* This case presents questions of law and fact common to all class  
6 members, which predominate over individualized issues. Those common questions include:

- 7 i. Whether UHC engaged in the wrongful conduct alleged herein;
- 8 ii. Whether the alleged conduct constitutes violations of the laws asserted;
- 9 iii. Whether UHC is a "provider of health care" under CAL. CIV. CODE § 56.101(a);
- 10 iv. Whether the information exposed in the breach was "medical information"  
11 under CAL. CIV. CODE § 56.101(a);
- 12 v. Whether UHC owed a duty to exercise reasonable care in maintaining medical  
13 information;
- 14 vi. Whether UHC exercised reasonable care with respect to its maintenance of  
15 Sensitive Information, including medical information;
- 16 vii. Whether UHC exercised reasonable care with respect to the data breach  
17 notification it sent to the Class;
- 18 viii. Whether UHC knew or should have known about the inadequacies of its data  
19 protection, storage, and security;
- 20 ix. Whether UHC failed to use reasonable care and commercially reasonable  
21 methods to safeguard and protect Plaintiffs' and the Class's Sensitive  
22 Information from unauthorized theft, release, or disclosure;
- 23 x. Whether the proper data security measures, policies, procedures and protocols  
24 were in place and operational within UHC's computer systems to safeguard and  
25 protect Plaintiff's and the Class's Sensitive Information from unauthorized  
26 theft, release or disclosure;
- 27 xi. Whether UHC's misconduct amounts to a violation of Cal. Bus. & Prof. Code §  
28 17200, *et seq.*;

- xii. Whether UHC's conduct was the proximate cause of Plaintiff's and the other Class member's injuries;
- xiii. Whether UHC took reasonable measures to determine the extent of the data breach after it was discovered;
- xiv. Whether UHC's negligence caused a legally cognizable injury to Plaintiff and the Class;
- xv. Whether UHC complied with the statutory and regulatory requirements for sending data breach notifications
- xvi. Whether Plaintiff and the Class are entitled to nominal damages under the Confidentiality of Medical Information Act;
- xvii. Whether Plaintiffs and the Class are entitled to recover actual damages and/or statutory damages; and
- xviii. Whether Plaintiff and the Class are entitled to other appropriate remedies, including injunctive relief.

62. *Typicality.* Plaintiff is a member of the proposed class because their medical information was exposed in the breach of UHC's network. Consequently, Plaintiff's claims are typical of the class he seeks to represent.

63. *Adequacy.* Plaintiff is an adequate class representative. He seeks relief for all members of the class and will put the interests of the class as a whole ahead of his individual interests. He has no conflicts of interest with any other member of the class. Additionally, Plaintiff has retained experienced counsel who have successfully prosecuted class actions, including data breach class actions, in California courts, as well as state and federal courts throughout the country.

**D. A class action is superior to individually litigating Class members' claims.**

64. Class-wide adjudication will produce substantial benefits for the Court and for litigants because joinder of all individual Class members is impracticable and inefficient, particularly when compared to the relatively small amount-in-controversy for most individual Class members.

65. Moreover, the prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications. As a result, class-wide adjudication presents

1 fewer management difficulties, conserves judicial resources and the parties' resources, and protects the  
2 rights of each Class member.

3 **CAUSES OF ACTION**

4 **COUNT I:**

5 **Negligence**

6 66. Plaintiffs incorporate by reference all preceding allegations.

7 67. Plaintiffs and Class members entrusted Defendant with highly sensitive and personal  
8 private data subject to confidentiality.

9 68. In obtaining and storing Plaintiffs' and Class members' information, Defendant owed a  
10 duty of reasonable care in safeguarding this information.

11 69. Defendant owed this duty to Plaintiffs and the Class because Plaintiffs and the Class are  
12 a well-defined, foreseeable, and probable group of individuals whom Defendant should have been  
13 aware could be injured by its inadequate security protocols and failure to promptly disclose the data  
14 breach. Defendant required Plaintiffs and the Class to provide it with their Sensitive Information as a  
15 condition of receiving medical treatment and, as part of its services, then took control and managed  
16 that Sensitive Information on behalf of its patients. The foreseeable harm to Plaintiffs and the Class of  
17 Defendant's inadequate data security measures created a duty to act reasonably in security Sensitive  
18 Information,

19 70. Defendant also owed a duty to timely and accurately disclose the scope, nature, and  
20 occurrence of the data breach. This disclosure is necessary so Plaintiff and the Class can take  
21 appropriate measures to avoid unauthorized use of their Sensitive Information, accounts, cancel and/or  
22 change usernames and passwords on compromised accounts, monitor their accounts to prevent  
23 fraudulent activity, contact their financial institutions about compromise or possible compromise,  
24 obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by  
25 the data breach and Defendant's unreasonable misconduct.

26 71. Defendant breached its duty to Plaintiff and the Class by failing to implement and  
27 maintain reasonable security controls that were capable of adequately protecting the Sensitive  
28 Information of Plaintiff and the Class.

1           72. Defendant also breached its duty to timely and accurately disclose to Plaintiff and the  
2 Class that their Sensitive Information had been or was reasonably believed to have been improperly  
3 accessed or stolen.

4           73. Defendant's networks, systems, protocols, policies, procedures and practices were not  
5 adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and  
6 class members' information was secured from release, disclosure, or publication.

7           74. Defendant's networks, systems, protocols, policies, procedures and practices were not  
8 reasonable given the sensitivity of the Plaintiffs' and class members' information.

9           75. Upon learning of the data breach, Defendant should have immediately reported the data  
10 breach to Plaintiff and Class members, credit reporting agencies, financial institutions, and all other  
11 third parties with a right to know and the ability to mitigate harm to Plaintiffs and Class members.

12           76. Despite knowing its networks, systems, protocols, policies, procedures and practices  
13 were not adequately designed, implemented, maintained, monitored and tested to ensure that  
14 Plaintiff's and class members' information were secured from release, disclosure, and publication,  
15 Defendants ignored the inadequacies and were unmindful of the risk of release, disclosure, and  
16 publication they had created.

17           77. Defendant's behavior evidences a reckless disregard for Plaintiff's and class members'  
18 rights. Defendant's negligence is directly linked to Plaintiff's and Class members' injuries.

19           78. As a result of Defendant's reckless disregard for Plaintiff's and class members' rights  
20 by failing to secure their information despite knowing their networks, systems, protocols, policies,  
21 procedures, and practices were not adequately designed, implemented, maintained, monitored, and  
22 tested, Plaintiff and class members suffered injury, including but not limited to the impermissible  
23 release, disclosure, and publication of their information, as well as exposure to a heightened, imminent  
24 risk of fraud, identity theft, financial and other harm.

25           79. The injuries to Plaintiff and the Class were reasonably foreseeable to Defendant  
26 because laws and statutes, and industry standards require it to safeguard and protect its computer  
27 systems and employ procedures and controls to ensure that unauthorized third parties did not gain  
28 access to Plaintiff's and the Class's Sensitive Information.

1 80. Those injuries were a proximate and reasonably foreseeable result of UHC's breach of  
2 its duty of reasonable care in safeguarding class members' information.

3 81. Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

4 **COUNT II:**

5 **Invasion of Privacy**

6 82. Plaintiff incorporates by reference all preceding allegations.

7 83. Under California law, defendants are liable for invasion of privacy if: (1) the plaintiff  
8 possessed a legally protected privacy interest, (2) in which the plaintiff maintained a reasonable  
9 expectation of privacy, and (3) the defendant's intrusion into that privacy interest was highly  
10 offensive. (*See, e.g., Hernandez v. Hillsides, Inc.* (2009) Cal. 4th 272, 287.)

11 84. UHC knew, or should have known, that its data security practices were inadequate and  
12 had numerous vulnerabilities.

13 85. UHC reckless or negligently failed to take reasonable precautions to ensure its data  
14 systems were protected.

15 86. UHC knew or should have known that its acts and omissions would likely result in a  
16 data breach, which would necessarily cause harm to Plaintiff and the Class.

17 87. The exposure of medical information is a highly offensive breach of social norms.

18 88. Plaintiff and the Class had a reasonable, legally protected privacy interest in their  
19 medical information.

20 89. As a result of UHC's acts and omissions, third parties accessed the medical records and  
21 other personal information of Plaintiff and the Class without authorization.

22 90. UHC is liable to Plaintiff and the Class for damages in an amount to be determined at  
23 trial.

24 **COUNT III:**

25 **Violations of the Confidentiality of Medical Information Act,**

26 **CAL. CIV. CODE § 56, et seq.**

27 91. Plaintiff incorporates by reference all preceding allegations.

28 92. Under Section 56.101, "[a]ny provider of health care . . . who negligently creates,

1 maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to  
2 the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” (CAL. CIV. CODE  
3 § 56.101, subdiv. a.) Section 56.36(b) provides that “an individual may bring an action against a  
4 person or entity who has negligently released confidential information or records concerning him or  
5 her in violation of this part, for either or both” actual damages and nominal damages of \$1,000. (CAL.  
6 CIV. CODE § 56.36, subdiv. b.)

7 93. A claim for “negligent release under section 56.36 does not require an affirmative  
8 communicative act but instead can be accomplished by negligently allowing information to end up in  
9 the possession of an unauthorized person.” (*Sutter Health v. Superior Court* (2014) 227 Cal. App. 4th  
10 1546, 1554–55.) Defendants are liable if their “negligence results in unauthorized or wrongful access  
11 to the [plaintiff’s] information.” (*Regents of Univ. of Cal. v. Superior Court* (2013) 220 Cal. App. 4th  
12 549, 554.)

13 94. UHC is a provider of health care.

14 95. UHC created, maintained, preserved, stored, abandoned, destroyed, and disposed of  
15 medical information regarding Plaintiff and the Class.

16 96. UHC was negligent because it failed to take reasonable precautions to ensure its data  
17 systems were protected.

18 97. As a result of UHC’s negligence, an unauthorized third-party gained wrongful access to  
19 the medical information of Plaintiff and the Class.

20 98. UHC is therefore liable for damages in an amount to be determined at trial, but not less  
21 than the statutorily provided nominal damages of \$1,000 for each class member.

22 **COUNT IV:**

23 **Violations of the Consumer Records Act,**

24 **CAL. CIV. CODE § 1798.80, et seq.**

25 99. Plaintiff incorporates by reference all preceding allegations.

26 100. Under California law, any “person or business that conducts business in California, and  
27 that owns or licenses computerized data that includes personal information” must “disclose any breach  
28 of the system following discovery or notification of the breach in the security of the data to any



1 resident of California whose unencrypted personal information was, or is reasonably believed to have  
2 been, acquired by an unauthorized person.” (CAL. CIV. CODE § 1798.2.) The disclosure must “be made  
3 in the most expedient time possible and without unreasonable delay” (*Id.*), but “immediately following  
4 discovery [of the breach], if the personal information was, or is reasonably believed to have been,  
5 acquired by an unauthorized person.” (CAL. CIV. CODE § 1798.82, subdiv. b.)

6 101. The data breach constitutes a “breach of the security system” of UHC.

7 102. An unauthorized person acquired the personal, unencrypted information of Plaintiff and  
8 the Class.

9 103. UHC knew that an unauthorized person had acquired the personal, unencrypted  
10 information of Plaintiff and the Class, but waited four months to notify them.

11 104. Two months was an unreasonable delay under the circumstances.

12 105. UHC’s unreasonable delay prevented Plaintiff from taking appropriate measures from  
13 protecting themselves against harm.

14 106. Because Plaintiff and the Class were unable to protect themselves, they suffered  
15 incrementally increased damages that they would not have suffered with timelier notice.

16 107. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be  
17 determined at trial.

18 **COUNT V:**

19 **Violations of the Unfair Competition Law,**

20 **BUS. & PROF. CODE § 17200, et seq.**

21 108. Plaintiff incorporates by reference all preceding allegations.

22 109. The Unfair Competition Law provides that:

23 “[U]nfair competition shall mean and include any unlawful, unfair or fraudulent business  
24 act or practice and unfair, deceptive, untrue or misleading advertising and any act  
25 prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of  
26 the Business and Professions Code.” (BUS. & PROF. CODE § 17200.)

27 110. Defendant stored the Sensitive Information of Plaintiff and the Class in its computer  
28 systems and knew or should have known it did not employ reasonable, industry standard, and

1 appropriate security measures that complied with applicable regulations and that would have kept  
2 Plaintiff's and the Class's Sensitive Information secure and prevented the loss or misuse of that  
3 Sensitive Information.

4 111. Defendant failed to disclose to Plaintiff and the Class that their Sensitive Information  
5 was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that  
6 Defendant had secured their Sensitive Information. At no time were Plaintiff and the Class on notice  
7 that their Sensitive Information was not secure, which Defendant had a duty to disclose.

8 112. Had Defendant complied with these requirements, Plaintiff and the Class would not  
9 have suffered the damages related to the data breach.

10 113. UHC's conduct was unlawful, in that it violated the Confidentiality of Medical  
11 Information Act and the Consumer Records Act.

12 114. UHC's conduct was also unfair, in that it violated a clear legislative policy in favor of  
13 protecting consumers from data breaches.

14 115. Defendant also engaged in unfair business practices under the "tethering test." Its  
15 actions and omissions, as described above, violated fundamental public policies expressed by the  
16 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all  
17 individuals have a right of privacy in information pertaining to them . . . The increasing use of  
18 computers . . . has greatly magnified the potential risk to individual privacy that can occur from the  
19 maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the  
20 Legislature to ensure that personal information about California residents is protected."); Cal. Bus. &  
21 Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy  
22 Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a  
23 violation of the law.

24 116. As a result of those unlawful and unfair business practices, Plaintiff and the Class  
25 suffered an injury-in-fact and have lost money or property.

26 117. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing  
27 benefit to consumers or competition under all of the circumstances.

28 118. There were reasonably available alternatives to further UHC's legitimate business

1 interests, other than the misconduct alleged in this complaint.

2 119. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of  
3 all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant  
4 because of its unfair and improper business practices; a permanent injunction enjoining Defendant's  
5 unlawful and unfair business activities; and any other equitable relief the Court deems proper.

6 **PRAYER FOR RELIEF**

7 Plaintiff, individually and on behalf of all others similarly situated, demands:

- 8 a. certification of the proposed Class;
- 9 b. appointment of the Plaintiff's counsel as class counsel;
- 10 c. actual and nominal damages in an amount to be determined at trial;
- 11 d. a declaration that UHC's conduct wrongful, unfair, unconscionable and in violation of  
12 California law;
- 13 e. an order enjoining UHC's unlawful and unfair conduct;
- 14 f. an award to Plaintiff and the Class of all damages, including attorneys' fees and  
15 reimbursement of litigation expenses, recoverable under applicable law; and
- 16 g. such other relief as this Court deems just and equitable.

17 **DEMAND FOR JURY TRIAL**

18 Plaintiff demands a jury trial on all applicable claims.

19  
20  
21  
22 Dated: January 18, 2022

Respectfully submitted,

By: \_\_\_\_\_

23 Michael J. Boyle, Jr. (SBN 258560)  
24 [mboyle@meyerwilson.com](mailto:mboyle@meyerwilson.com)

25 MEYER WILSON CO., LPA  
26 Matthew R. Wilson, Esq. (SBN 290473)  
27 [mwilson@meyerwilson.com](mailto:mwilson@meyerwilson.com)  
305 W. Nationwide Blvd  
Columbus, OH 43215  
Phone Number: 614-224-6000  
28 Fax: 614-224-6066

# EXHIBIT 1

## Internet & Dark Web Monitoring

Scans online sources known for illegally buying and selling personal information, such as your Social Security number, and notifies you if your identity may be at risk.

**Notifications** 12 NEW

Page: 1 ◀ 1 2 ▶

Type	Date	Actions
<span style="color: red; font-weight: bold;">Internet &amp; Dark Web Monitoring</span>	12/21/2021	<span style="color: red; font-weight: bold;">✕</span>
<span style="color: red; font-weight: bold;">Internet &amp; Dark Web Monitoring</span>	12/21/2021	<span style="color: red; font-weight: bold;">✕</span>
<span style="color: red; font-weight: bold;">Internet &amp; Dark Web Monitoring Report</span>	12/08/2021	<span style="color: red; font-weight: bold;">✕</span>

### Compromised Social Security Number

⚠ **Compromised Social Security Number:** \*\*\*-\*\*-8593  
**Date Found:** 10/07/2021

We've found a match to your Social Security Number (SSN) online. Below you will find additional information on next steps to take to ensure your personal information is secure.

#### Additional Info

The following data was found compromised with your SSN.

<b>First Name</b>	NAREK	<b>Records Found On</b>	10/07/2021
<b>Last Name</b>	AVETISYAN	<b>D.O.B.</b>	D.O.B. FOUND
<b>Social Security Number</b>	***-**-8593	<b>Found With</b>	SOCIAL SECURITY NUMBER
<b>Potential Site</b>	UNITEDHEALTHCENTERS.ORG		

Here's what to do:

- Contact Identity Champion at 1-844-IDCHAMP (844-432-4267). We'll help you determine if an identity theft event has occurred and guide you through any necessary restoration activities. We may assist you with the following activities:
  - Review your credit report for indications of identity theft
  - Place a fraud alert or security freeze with the three credit bureaus
- As a precaution, keep an eye on your accounts for unfamiliar transactions.

### Compromised Phone & Compromised Social Security Number

⚠ **Compromised Phone Numbers:** (559)  
**Compromised Social Security Number:** \*\*\*-\*\*-8593  
**Date Found:** 10/07/2021

We have detected your personal info on a risky website.

- We have detected your personal info on a risky website.
- We've found a match to your Social Security Number (SSN) online. Below you will find additional information on next steps to take to ensure your personal information is secure.

#### Additional Info

The following data was found compromised with your SSN.

<b>First Name</b>	NAREK	<b>Phone Number</b>	(559)
<b>Last Name</b>	AVETISYAN	<b>Social Security Number</b>	***-**-8593
<b>Address 1</b>	450 W SAMPLE AVE		
<b>City</b>	FRESNO		
<b>State</b>	CA		
<b>Zip</b>	937041419		
<b>Potential Site</b>	UNITEDHEALTHCENTERS.ORG		
<b>Records Found On</b>	10/07/2021		
<b>D.O.B.</b>	D.O.B. FOUND		
<b>Found With</b>	IDHOMEPHONE_IDSSN		

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

2. Here's what to do: 1. Contact Identity Champion at 1-844-IDCHAMP (844-432-4267). We'll help you determine if an identity theft event has occurred and guide you through any necessary restoration activities. We may assist you with the following activities:

- Review your credit report for indications of identity theft
- Place a fraud alert or security freeze with the three credit bureaus

2. As a precaution, keep an eye on your accounts for unfamiliar transactions.

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 07/13/2020

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 07/13/2020

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 10/08/2020

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 12/09/2020

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 01/30/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 02/01/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 02/05/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 03/17/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 06/11/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 10/12/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

### Compromised Phone

⚠ **Compromised Phone Numbers:** (559)  
**Date Found:** 10/12/2021

We have detected your personal info on a risky website.

Here's what to do:

- Have you been receiving suspicious phone calls? If not, keep an eye out as you may receive additional identity alerts related to this incident. If you have been receiving suspicious calls, register your phone number at [www.donotcall.gov](#) or call 1-888-382-1222.
- For added security, you can have a password or code when calling financial institutions.
- Consider blocking unknown numbers that you feel are harassing you. In severe cases, you may need to change your number. Some phone companies may waive the fee. Call your phone service provider for more details.

If you have further questions, please feel free to contact us at 1-844-IDCHAMP (844-432-4267)

**Monitored Information**

#### Email Address (3/10) Why monitor this?

Add Email Address

1.	an**ek@me.com (Primary)	
2.	8n**ek@gmail.com	✕
3.	bu*****ek@gmail.com	✕

#### Social Security Number (1/1) Why monitor this?

1.	XXX-XX-XXXX (Primary)
----	-----------------------

#### Phone (1/10) Why monitor this?

Add Phone

1.	*****0969 (Primary)
----	---------------------

#### Credit/Debit Card (0/10) Why monitor this?

Add Credit/Debit Card

#### Bank Account (0/10) Why monitor this?

Add Bank Account

#### Driver's License (1/1) Why monitor this?

1.	Issuing State: CA	
	Driver's License Number: ****7993	✕

#### Passport (0/1) Why monitor this?

Add Passport

#### Retail or Membership Cards (0/10) Why monitor this?

Add Retail or Membership Cards


#### Medical ID (0/10) Why monitor this?

Add Medical ID

**Identity Champion presents**

**Compromised Email**

⚠ **Hacked Email: What to Do | Fed...**



**Hacked Email: What to Do**  
 The FTC gives you the inside scoop on what to do if your email is compromised.

**FAQs**

Expand All

- Where does Internet & Dark Web Monitoring's data come from?
- What time range does my initial Internet & Dark Web Monitoring report cover?
- What does it mean when I receive an alert?
- What if the alert references only some of the personal information Internet & Dark Web Monitoring is tracking?
- Is the buying and selling of others' personal information online illegal?
- Can I still become a victim of identity theft even though I am enrolled in Internet & Dark Web Monitoring?