IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS AT KANSAS CITY

JEREMY KRANT, TODD DEATON, THOMAS NASH, SHANA VACHHANI and KIMBERLY MILLER, individually and on behalf of all others similarly situated, Plaintiffs, v. UNITEDLEX CORPORATION, Defendant.	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Jeremy Krant, Todd Deaton, Thomas Nash, Shana Vachhani, and Kimberly Miller ("Plaintiffs"), by and through their undersigned counsel, bring this Class Action Complaint against Defendant UnitedLex Corporation ("ULX" or "Defendant") individually and on behalf of all others similarly situated, and allege as follows, based upon personal knowledge as to themselves, and upon information and belief as to all other matters.

INTRODUCTION

1. ULX is a Kansas-based company that provides data management and professional services to law firms and corporate legal departments in the areas of litigation and investigations, intellectual property, contracts, compliance, and legal operations. ULX specializes in technology-intensive litigation-support services and makes recommendations to clients on how to secure their data and how to respond in case of a breach.[1]

[1] UNITEDLEX, https://web.archive.org/web/20230601224209/https://unitedlex.com/litigation-and-investigations/incident-response/ (last visited Sept. 28, 2023).

2. On or before March 6, 2023, ULX suffered a data breach whereby third-party hackers gained access to over 200 GB of sensitive information maintained on ULX's servers and demanded a ransom in exchange for not releasing the information (the "Data Breach"). The stolen information included, at a minimum, full names, Social Security numbers, financial information used for payroll, and benefits information for ULX's current and former employees.

3. The stolen information also included the names and Social Security numbers of current and former employees' dependents (referred to herein as "PII").[2] Additionally, the hackers reported that they gained access to confidential and proprietary information for ULX's clients.

4. After ULX failed to meet the hackers' demands, the stolen information was released on an underground portion of the internet known as the dark web, where anyone with an internet browser can access and misuse it at their discretion. ULX did its best to cover up the breach, disclosing it only after dozens of victims reported suffering identity theft and fraud—and after the hackers publicly disclosed its existence.

5. Individuals impacted by the Data Breach are now at serious risk of continuing injury caused by the theft of their PII, which is in the possession of cybercriminals seeking to profit from it, and also freely available on underground websites for anyone to access. It is not surprising that dozens of victims have already reported suffering tax fraud, bank fraud, and other types of identity theft that will continue to haunt them for years to come.

[2] ULX noted dependent information was at risk if that information was provided to ULX.

6. ULX's CEO Daniel Reed publicly referred to the breach as a "non-event,"[3] which is demonstrably false given the number of people impacted and calamitous effects the Data Breach has already had on its victims. Mr. Reed stepped down as CEO in September 2023.[4]

7. ULX is responsible for the Data Breach because it failed to implement and maintain reasonable safeguards to protect its current and former employees' PII, as well as clients' confidential information. ULX knew better as its entire business is centered on handling sensitive information and counseling clients about implementing best practices to avoid such a breach.

8. Plaintiffs bring this action, on behalf of themselves and those similarly situated, to seek redress for the lifetime of harm they will now face, including reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, and the costs of extended credit monitoring services and identity-theft insurance.

9. Plaintiffs further seek injunctive relief requiring Defendant to implement and maintain reasonable data security practices going forward.

PARTIES

10. Plaintiff Jeremy Krant is a resident and citizen of Los Angeles, California.

11. Plaintiff Todd Deaton is a resident and citizen of Greenwood, Missouri.

12. Plaintiff Thomas Nash is a resident and citizen of Richmond, Virginia. He's the father of a minor child whose personal information may have been stolen during the Data Breach.

13. Plaintiff Shana Vacchani is a resident and citizen of Minneapolis, Minnesota.

---

[3] Steven Lerner, "UnitedLex Says Hello to Innovation, Goodbye to Some Staff," LAW360 (June 27, 2023), https://www.law360.com/pulse/articles/1693557 (subscription required) (last visited Sept. 28, 2023).

[4] On May 20, 2023, a document preservation letter was sent to ULX's in-house counsel Eric Kelly. Mr. Kelly acknowledged receipt of the letter on May 25, 2023.

14. Plaintiff Kimberly Miler is a resident and citizen of Jekyll Island, Georgia.

15. Defendant is a Delaware corporation with its principal place of business located at 11501 Sprint Pkwy., Overland Park, Kansas 66211.

JURISDICTION & VENUE

16. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because this is a class action in which at least one member of the Class is a citizen of a state different from Defendant, the amount in controversy exceeds $5 million exclusive of interest and costs, and the proposed Class contains more than 100 members.

17. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(2) and (c)(2) because a substantial part of the events or omissions giving risk to the claim occurred here and Defendant is subject to this Court's personal jurisdiction. Among other things, ULX is headquartered in this District, conducts substantial business operations in this District, and purposely availed themselves of the benefits of the Court's jurisdiction.

FACTUAL ALLEGATIONS

UnitedLex's Data-Security Expertise and Privacy Practices

18. Founded in 2006, ULX markets itself as a leader in legal innovation. As a private company, ULX has over 3,000 employees serving more than 400 customers worldwide with consulting services, litigation support, project management, law-firm solutions, intellectual property, data hosting, and legal staffing.[5] The hallmark of ULX's business is data security. ULX has leveraged security services, security certification, and has assembled an experienced executive leadership team to provide a high level of data security to its clients.

19. In 2015, ULX launched its Managed Security Service, which it pitched to clients

[5] UNITEDLEX, https://web.archive.org/web/20230607183809/https://unitedlex.com/about-unitedlex/ (last visited Sept. 28, 2023).

as including fully managed security operations and event monitoring, continuous cyber-risk management, threat-intelligence sharing, and on-call incident responders to deliver rapid response services in the event of a data breach.[6]

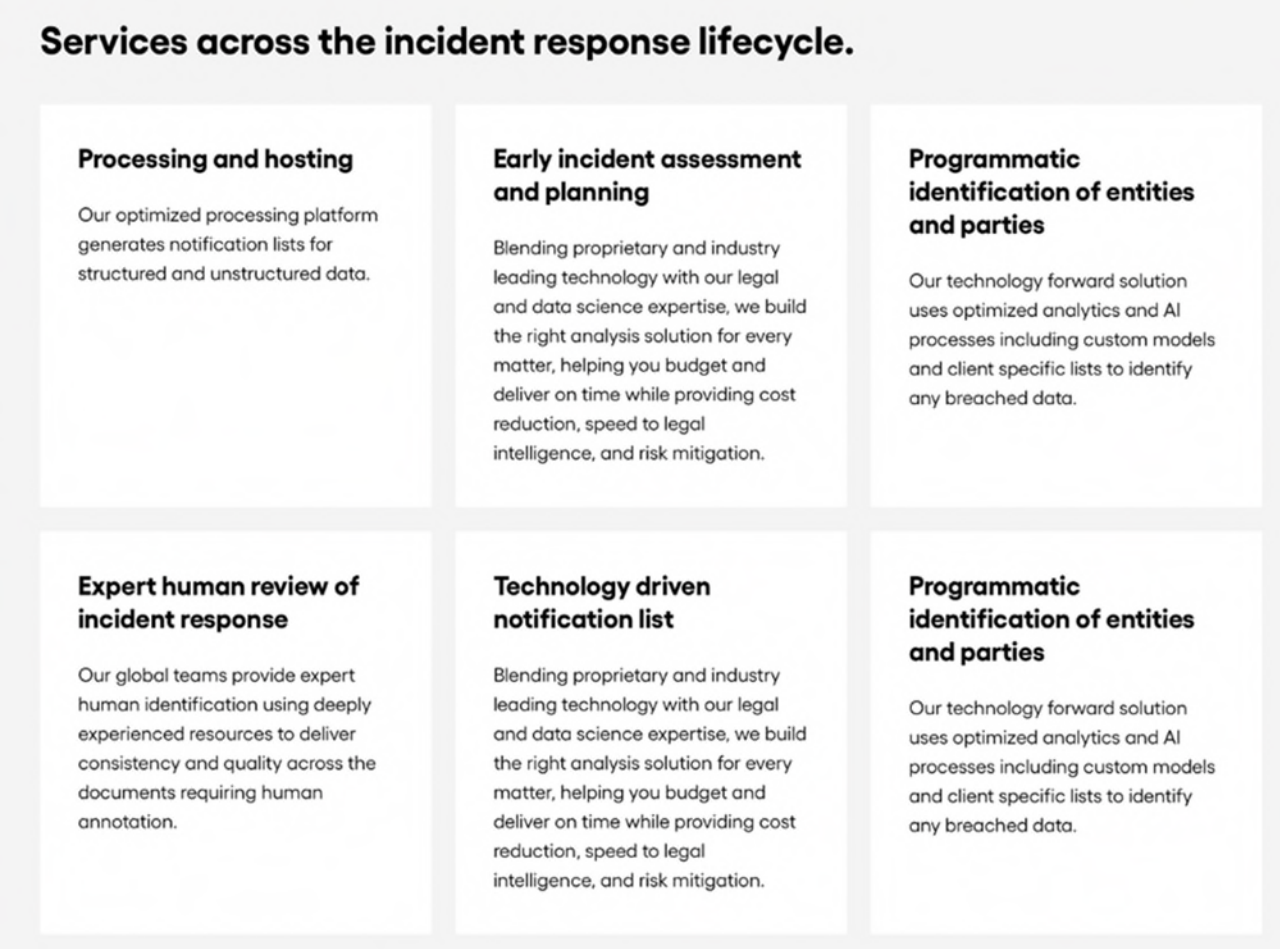
20. In 2016, ULX integrated with Securonix's security-analytics platform to broaden its cybersecurity threat-detection capabilities and reduce the time between a breach and its detection.[7]

21. ULX's website features a robust library of articles that highlight the importance of data security and how to prevent and respond to a data breach.[8] One article, entitled "Do You Know Where Your Company's Data Is?,"[9] explains that data breaches at major corporations have become "commonplace." The article stresses the importance of ensuring the security of data located with a third-party service provider and states that "the standard of care with regard to the protection of private information is rising, and ignorance is no longer an acceptable defense in the wake of a poorly managed cyberattack."[10]

22. Defendant's claimed proficiencies within incident response are highlighted on its website and reproduced below:[11]

---

[6] INSIGHTSSUCCESS, *UnitedLex Redefines Managed Security by Integrating Legal and Compliance Intelligence* (Apr. 21, 2015), https://www.insightssuccess.in/unitedlex-redefines-managed-security-by-integrating-legal-and-compliance-intelligence/ (last visited Sept. 28, 2023).
[7] CIO REVIEW, "UnitedLex Partners with Securonix to Streamline its Cyber Threat Detection Capabilities" (Sept. 26, 2016), https://www.cioreview.com/news/unitedlex-partners-with-securonix-to-streamline-its-cyber-threat-detection-capabilities-nid-22240-cid-29.html (last visited Sept. 28, 2023).
[8] *See* search of "data breach" on ULX website: https://unitedlex.com/?s=Data+Breach (last visited Sept. 28, 2023).
[9] UNITEDLEX, https://web.archive.org/web/20230607085201/https://unitedlex.com/insights/do-you-know-where-your-companys-data-is/ (last visited Sept. 28, 2023).
[10] *Id*.
[11] UNITEDLEX, https://web.archive.org/web/20230601224209/https://unitedlex.com/litigation-and-investigations/incident-response/ (last visited Sept. 28, 2023).



23. ULX's past and present executive leadership highlight their impressive experience with data security. For example, Josh Hass is the leader of ULX's cyber- discovery and incident-response practice. His biography emphasizes his experience working on "numerous data breach engagements ranging from business email compromise, data extortion, ransomware negotiation and recovery . . . ."[12]

24. ULX's Vice President of Information Technology from July 2020 to January 2023, Maurice Smith, gained experience with cyber security and intelligence in the United States Army.

[12] UNITEDLEX, https://web.archive.org/web/20230607101148/https://unitedlex.com/about-unitedlex/leadership/josh-hass/ (last visited Sept. 28, 2023).

He brought his impressive resume to ULX with a goal to "take security seriously not as a cliché, but through action."[13]

25. ULX's Chief Privacy Officer from October 2013 to December 2019, Jason Straight, spoke frequently about data privacy, cybersecurity, and data-breach response.[14] In a March 9, 2019 presentation, Mr. Straight presented at the RSA conference "Ransom: A Real-World Case Study in Data Theft, Forensics and the Law."[15] Those attending the presentation learned "the need for incident planning/response mechanisms" and "the steps to protect your organization's critical data and IP from both internal and external threats."[16] At this same conference, Mr. Straight presented on emerging threats, which included ransomware.

26. ULX integrated the importance of data security into its Privacy Policy, which states security is a "high priority" and ULX has "implemented appropriate administrative, technical and physical safeguards to prevent unauthorized access, use or disclosure" of PII and confidential information. ULX states that it requires "the same high standard of information security and information management" of any third parties it shares data with.[17]

27. By obtaining, collecting, and storing the PII and Confidential Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting this data from unauthorized disclosure.

---

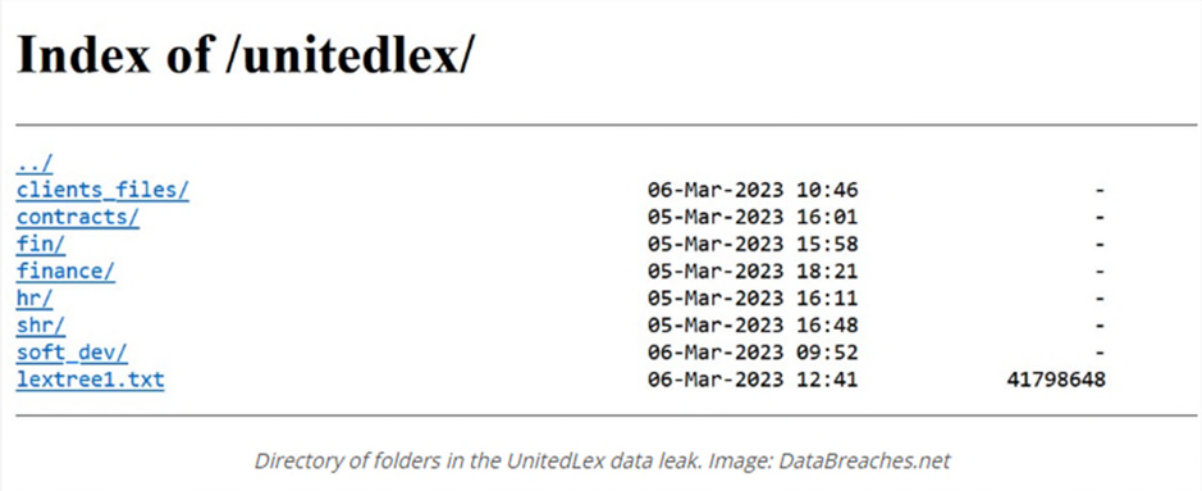
[13] UNITEDLEX, https://web.archive.org/web/20230329204401/https://unitedlex.com/news/we-are-unitedlex-maurice-smith/ (last visited Sept. 28, 2023).
[14] RSACONFERENCE, https://www.rsaconference.com/experts/jason-straight (last visited Sept. 28, 2023)
[15] RSACONFERENCE, https://www.rsaconference.com/Library/presentation/USA/2019/ransom-a-realworld-case-study-in-data-theft-forensics-and-the-law (last visited Sept. 28, 2023).
[16] *Id.*
[17] *Id.*

The Data Breach

28. On or before March 6, 2023, a ransomware group called d0nut accessed ULX's internal servers and seized control of over 200 GB of ULX's files. After d0nut gained access, the hackers alerted ULX as to the information they were able to access, which included PII.[18] The hackers sought payment in exchange for the release of this information.

29. On approximately April 4, 2023, d0nut contacted the website operators of DataBreaches.net ("DataBreaches") to publicize its hack of ULX. In a statement, d0nut confirmed "they downloaded over 200GB of data from UnitedLex's network, including confidential files involving payments, contracts, and other details related to numerous organizations and individuals."

30. DataBreaches reported that the information accessed included confidential and proprietary files, including personnel-related files. A screenshot of the directory of folders housing the leaked ULX data is reproduced below:[19]



Index of /unitedlex/

../		
clients_files/	06-Mar-2023 10:46	-
contracts/	05-Mar-2023 16:01	-
fin/	05-Mar-2023 15:58	-
finance/	05-Mar-2023 18:21	-
hr/	05-Mar-2023 16:11	-
shr/	05-Mar-2023 16:48	-
soft_dev/	06-Mar-2023 09:52	-
lextree1.txt	06-Mar-2023 12:41	41798648

Directory of folders in the UnitedLex data leak. Image: DataBreaches.net

[18] DATABREACHES, https://www.databreaches.net/unitedlex-hit-by-d0nut-ransomware-team-200-gb-of-corporate-files-leaked/ (last visited Sept. 28, 2023).
[19] Id.

31. Regarding the ransom, a spokesperson from d0nut told DataBreaches: "[t]hrough [the] negotiation process with United Lex's top management, we found out that most of their money [was] stored in Silicon Valley Bank. We also found an insurance with cybercrime coverage, but they refused to use this option. The sum we offered them to pay was $600,000,[20] which is significantly lower than their insurance limit."[21]

32. DataBreaches reported that d0nut reached out to one of ULX's clients, DXC, for a ransom and uploaded thirty-five DXC files to a file-sharing site.

33. DataBreaches reached out to ULX for comments about the Data Breach and received the following response:

> The security and integrity of our systems are of the utmost importance to us. We recently discovered suspicious activity on our network, immediately initiated our incident response protocols, engaged third-party forensic experts to determine the nature and scope of the activity, and notified the FBI.
>
> [ctd.]
>
> Our systems are fully operational, and we have been in constant contact with our customers and employees about this incident and our investigation.[22]

34. ULX's statement echoed those of CEO Daniel Reed, who was quoted in a June 2023 article as claiming that ULX had "notified all impacted parties."[23]

35. In direct conflict with ULX's public statements, ULX was not in constant contact with those affected and did not notify former employees affected until July 11, 2023, **at least four months after ULX learned of the breach**.[24]

---

[20] According to DataBreaches, at some point the ransom increased to $5 million.
[21] DATABREACHES.COM, *supra* note 18.
[22] *Id*.
[23] Lerner, *supra* note 3.
[24] At some point after the Data Breach, ULX notified, via email, current employees , as well as clients; the contents of those notifications will be sought in discovery.

36. On July 11, 2023, ULX finally notified former employees, via letter, that their information was accessed, but its correspondence withheld critical information regarding the nature of the Data Breach and the ransom demand(s):

> UnitedLex is writing to notify you of a recent data security incident. Although our investigation is ongoing, we have determined that your personal information was most likely impacted. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to help protect your information and resources we are making available to help you.
>
> **What happened:**
> On March 6, 2023, UnitedLex discovered suspicious network activity immediately implemented its incident response protocols, and engaged cybersecurity experts to assist with determining what occurred and whether any data was compromised. The investigation found that an unauthorized actor gained access to the UnitedLex corporate environment and took some data stored on tie system. We are in the process of working with a vendor to review this data to identify what personal information, specifically, may have been impacted.
>
> **What information was involved:**
> The information stored in the system may have included a combination of the following: your name, Social Security number, financial account number for payroll purposes, and benefits information. If you provided. UnitedLex with information for your dependents, such as names and Social Security numbers, this information may also have been affected.
>
> **What we are doing:**
> We have taken steps to secure our system, such as changing all passwords, deploying additional 24/7 system monitoring, and conducting a thorough investigation. We have arranged for you to receive identity monitoring services offered by Kroll at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.
>
> Your identity monitoring services from Kroll will include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.
>
> **What you can do:**
> Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also regularly review your credit reports and financial statements, and immediately report any suspicious activity.

37. This letter was deficient in multiple ways. First, the letter failed to disclose the cause of the breach, full scope of information compromised, and the timeline associated with the breach.

38. Second, the letter omitted altogether that the group behind the hack was a ransomware group that released the PII to the dark web.

39. Third, the letter downplayed the harm associated with the breach by failing to disclose that ULX employees had already reported being victimized with instances of tax fraud and identify theft.

40. Further, ULX did not apologize for the breach or provide any explanation for why it took them so long to notify individuals of the breach.

41. The letter promised "identify monitoring services" for twenty-four months for former employees through Kroll, a vastly inadequate protection given the lifetime of harm affected individuals now face. Also, the monitoring offered was not extended to family and dependents even though the letter expressly mentions dependents may have been affected by the Data Breach.

42. ULX touts its ability to leverage technology and global teams to help clients respond to a cyber incent; comply with various regulations relating to notice;[25] and thereby respond to a data-security incident with "confidence, speed and precision."[26]

43. It is inexcusable that a company with this level of sophistication relative to cyber threats and notification of impacted parties would issue a notice that was not only dilatory but also incomplete as to multiple material aspects of the Data Breach.

---

[25] UNITEDLEX, https://web.archive.org/web/20230607095512/https://unitedlex.com/insights/cyber-incident-response/ (last visited Sept. 28, 2023).

[26] UNITEDLEX, https://web.archive.org/web/20230601224209/https://unitedlex.com/litigation-and-investigations/incident-response/ (last visited Sept. 28, 2023).

The Data Breach Was Preventable

44. Following the Data Breach, ULX stated it was "changing all passwords, deploying additional 24/7 system monitoring and conducting a thorough investigation."

45. But ULX, like any company its size storing valuable data, should have had strong protections in place to detect and terminate a successful intrusion long before access and exfiltration of 200 GB of confidential files. ULX's implementation of enhanced security measures only after the fact is inadequate given its knowledge that it was a prime target for cyberattacks.

46. It is well-known that use of stolen credentials has long been the most popular and effective method of gaining unauthorized access to a company's internal networks and that organizations should activate defenses to prevent such attacks.

47. According to the FBI, phishing schemes designed to induce the disclosure of user credentials were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[27]

48. According to Verizon's 2021 *Data Breach Investigations Report*, 43% of breaches stemmed from phishing and/or pretexting schemes.[28]

49. There are two primary ways to mitigate the risk of stolen credentials: user education and technical security barriers. User education is the process of making employees or other users of a network aware of common disclosure schemes and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients.

---

[27] FBI INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Sept. 28, 2023).

[28] VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited Sept. 28, 2023).

50. For example, a common phishing e-mail is an "urgent" request from a company "executive" requesting confidential information in an accelerated timeframe. The request may come from an e-mail address that appears official but contains a different number or letter. Other phishing methods include baiting a user to click a malicious link that redirects them to a nefarious website or download an attachment containing malware.

51. User education provides the easiest method to assist in properly identifying fraudulent "spoofing" e-mails and prevent unauthorized access of sensitive internal information. According to September 2020 guidance from the Cybersecurity and Infrastructure Security Agency ("CISA"), organizations housing sensitive data should "[i]mplement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity" and conduct "organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails."[29]

52. From a technical perspective, companies can also greatly reduce the flow of phishing e-mails by installing software that scans all incoming messages for harmful attachments or malicious content and implementing certain security protocols governing e-mail transmissions, including Sender Policy Framework ("SPF"), DomainKeys Identified Mail ("DKIM"), and Domain-based Message Authentication, Reporting and Conformance ("DMARC").

53. Additionally, because the goal of many phishing attempts is to gain an employee's login credentials in order to access a company's network, there are industry-standard measures that companies can implement to greatly reduce unauthorized access—even if a phishing attempt is successful. For example, multi-factor authentication is a security system that requires more than

[29] CYBERSECURITY AND INFRASTRUCTURE AGENCY, *Ransomware Guide* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf (last visited Sept. 28, 2023).

one method of authentication from independent categories of credentials to verify the user's identity for a login. This could include entering a code from the user's smartphone, answering a security question, or providing a biometric indicator such as a fingerprint or facial recognition—in addition to entering a username and password. Thus, even if hackers obtain an employee's username and password, access to the company's system is thwarted because they do not have access to the additional authentication methods.

54. Similarly, companies housing sensitive data must implement adequate "network segmentation," which is the practice of dividing a larger network into several smaller subnetworks that are each isolated from one another to provide enhanced security. For example, hackers that gain access to an unsegmented network (commonly through phishing) can move laterally across the network to access databases containing valuable assets, such as sensitive personal information or financial records. Malicious lateral movement can be difficult to detect because it oftentimes appears as normal network traffic. By implementing adequate network segmentation, companies can prevent even those hackers who already gained a foothold in their network from moving across databases to access their most sensitive data.

55. Network segmentation is commonly used in conjunction with the principle of least privilege ("POLP"), which is a security practice that limits employees' privileges to the minimum necessary to perform the job or task. In an IT environment, adhering to POLP reduces the risk of hackers gaining access to critical systems or sensitive data by compromising a low-level user account, device, or application.[30] In an example given by security software provider Digital Guardian:

[30] DIG. GUARDIAN, https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (last visited Sept. 28, 2023).

> [A]n employee whose job is to enter info into a database only needs the ability to add records to that database. If malware infects that employee's computer or if the employee clicks a link in a phishing email, the malicious attack is limited to making database entries. If that employee has root access privileges, however, the infection can spread system-wide.[31]

56. This is precisely why approximately 67% of targeted malware and stolen-credential schemes are directed at individual contributors and lower-level management personnel.[32]

57. In addition to mitigating the risk of stolen credentials, CISA guidance encourages organizations to prevent unauthorized access by:

- Conducting regular vulnerability scanning to identify and address vulnerabilities, particularly on internet-facing devices;
- Regularly patching and updating software to the latest available versions, and prioritizing timely patching of internet-facing servers and software processing internet data;
- Ensuring devices are properly configured and that security features are enabled;
- Employing best practices for use of Remote Desktop Protocol ("RDP") as threat actors often gain initial access to a network through exposed and poorly secured remote services; and
- Disabling the operating system network file-sharing protocol known as Server Message Block ("SMB"), which is used by threat actors to travel through a network to spread malware or access sensitive data.[33]

58. CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time

---

[31] Id.
[32] HEALTH IT SEC., https://healthitsecurity.com/news/pharmaceutical-companies-most-targeted-industry-by-cybercriminals (last visited Sept. 28, 2023).
[33] Ransomware Guide, *supra* note 29, at 4.

intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[34]

59. Despite being responsible for highly sensitive data, ULX did not adhere to these best practices. Its implementation of some or all of these measures after the fact is inexcusable given ULX's knowledge of the sensitivity of the data it was housing, which made it a prime target for cyberattacks.

60. As emphasized above, ULX markets itself as a data-security company that protects third-party data for clients and assists its clients in responding to data breaches. ULX did not heed its own advice to ensure the third-party data it obtained, collected, and stored was secure from a hack.

61. Legal-services entities like Defendant are prime targets because of the information they collect and store, including intellectual property, proprietary information, and personal information of employees and patients—all extremely valuable on underground markets. Although ULX is not a law firm, it is hired by law firms to house, monitor, and secure highly confidential information and data.

62. A January 2023 article featured in *The American Lawyer* and republished in multiple other online resources stated the "new school of cybercrime has been far more effective at targeting law firms large and small since the onset of Covid-19."

63. Chris Loehr, Executive Vice President of cybersecurity consulting firm Solis Security, stated, "[l]aw firms frequently don't understand how much client and personal data they

[34] *Id*. at 5.

have until they've been hacked." In the article, Loehr recommends the tracking and disposal of unnecessary data as being "crucial."[35]

64. ULX observed frequent public announcements of data breaches affecting legal-services entities and knew that information of the type it collected, maintained, and stored was and is highly coveted and a frequent target of hackers. Likewise, a 2019 article published by the American Bar Association stated that more than 100 law firms have report data breaches since 2014.[36]

65. For example, in June 2017, DLA Piper suffered a ransomware attack that prevented its employees worldwide from using firm telephones or email systems while restricting access to certain documents.[37]

66. Further, in 2017, Jenner & Block fell victim to a phishing scheme resulting in the inadvertent sharing of confidential information, including Social Security numbers and salaries.[38]

67. In March 2020, Epiq Global, a legal-services provider and ULX competitor, disclosed it had been subjected to a massive ransomware attack where its systems were infected

[35] Dan Roe, "Cyberattacks 'Inevitable' for Law Firms, Highlighting Need for Comprehensive Incident Response Plans," *The American Lawyer* (Jan. 10, 2023), https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/?slreturn=20230210143819 (last visited Sept. 28, 2023).
[36] Debra Cassens Weiss, "More than 100 Law Firms Have Reported Data Breaches; 2 BigLaw Firms Affected," *ABA Journal* (Oct. 18, 2019), https://www.abajournal.com/news/article/more-than-100-law-firms-have-reported-data-breaches-2-biglaw-firms-affected (last visited Sept. 28, 2023).
[37] LAW.COM, https://www.law.com/international-edition/2017/06/27/dla-piper-hit-by-cyber-attack-with-phones-and-computers-down-across-the-firm/ (last visited Sept. 28, 2023).
[38] ABA JOURNAL, https://www.abajournal.com/news/article/more-than-100-law-firms-have-reported-data-breaches-2-biglaw-firms-affected (last visited Sept. 28, 2023).

with the TrickBot malware, which is most commonly spread through phishing emails.[39]

68. In May 2020, Grubman Shire Meiselas & Sacks, a firm that offers legal services to the entertainment and media industries, suffered a ransomware attack involving leaked information about a celebrity client. The hackers threatened to release information involving other celebrities; much of the information remains accessible on underground markets.[40]

69. In November 2022, a data breach occurred at the law firm of Cadwalader, Wickersham & Taft whereby an unauthorized party gained remote access to the firm's systems and acquired information from the firm's network. The data breach resulted in the firm having to "wipe firm-issued laptop hard drives" and it "forced many of its internal systems offline."[41]

70. In addition to these cyberattacks targeting the legal industry, ULX observed numerous well-publicized data breaches involving major corporations in other industries that were targeted given the sensitive consumer information they held. For example, through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when users' names, addresses, and dates of birth were stolen as part of a multi-faceted cyberattack.[42]

---

[39] BLEEPING COMPUTER, Lawrence Abrams, "Ryuk Ransomware Attacked Epiq Global Via TrickBot Infection" (Mar. 4, 2020), https://www.bleepingcomputer.com/news/security/ryuk-ransomware-attacked-epiq-global-via-trickbot-infection/ (last visited Sept. 28, 2023).

[40] ARCTIC WOLF, "The Top 10 Legal Industry Cyber Attacks" (July 10, 2023), https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/ (last visited Sept. 28, 2023).

[41] BLOOMBERG LAW, Meghan Tribe, "Cadwalader Hit with Class Action Stemming from Data Breach" (Apr. 12, 2023), https://news.bloomberglaw.com/business-and-practice/cadwalader-hit-with-class-action-stemming-from-data-breach (last visited Sept. 28, 2023).

[42] CNN, Selena Larson, "Every Single Yahoo Account was Hacked – 3 Billion in All" (Oct. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (last visited Sept. 28, 2023).

71. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment-card systems at Target and the Home Depot. Both breaches led to rampant payment-card fraud and other damages, to both consumers and the card-issuing banks.[43]

72. In September 2017, credit-reporting agency Equifax announced that hackers stole the personal and financial information of 147 million Americans between May and July 2017.[44]

73. The following year, hotel giant Marriott announced that 383 million guest records were exfiltrated from its hotel guest reservation database over a four-year period.[45]

74. Despite being a holder of highly sensitive information, ULX failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access on its network.

75. Defendant had the knowledge and resources to prevent a breach, making significant expenditures to promote its business operations but neglecting to adequately invest in data security, despite the growing number of well-publicized data breaches affecting the legal, and other, industries.

The Effects of the Data Breach on Impacted Individuals

76. Given the highly sensitive nature of the PII stolen during the Data Breach, and its subsequent publication on underground websites, fraudsters across the globe have the ability to

[43] KREBSONSECURITY, "Home Depot Hit By Same Malware as Target" (Sept. 7, 2014), https://krebsonsecurity.com/tag/home-depot-databreach/ (last visited Sept. 28, 2023).
[44] EQUIFAX, Equifax 2017 Cybersecurity Incident & Important Consumer Information, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 28, 2023).
[45] MARRIOTT INT'L, "Marriott Provides Update on Starwood Database Security Incident," (Jan. 4, 2019), https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/ (last visited Sept. 28, 2023).

commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class members, both currently and on an indefinite, prospective basis.

77. In fact, many of its victims have already reported significant harms as a direct result of the Data Breach, including identity theft, financial fraud, tax fraud, and unauthorized financial accounts or lines of credit being opened in their names.

78. Plaintiffs and Class members have also spent time and money dealing with the Data Breach's fallout, including by purchasing credit-protection services, checking credit reports, and expending effort searching for unauthorized activity.

79. Further, the impacts of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to obtain credit, such as student loans, mortgages, and credit cards.[46]

80. It is no wonder, then, that identity theft exacts a severe emotional toll on its victims. A 2022 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft, including:

- 84% of respondents reported feeling worried or anxious;
- 76% reported feeling violated;
- 65% reported feeling vulnerable;
- 57% reported feeling sad or depressed; and

[46] IDENTITY THEFT RES. CTR., *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Sept. 28, 2023).

- 10% reported feeling suicidal.[47]

81. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft, including:

- 90% of respondents reported sleep problems;
- 87% experienced heightened stress;
- 57% reported changes in eating or drinking habits;
- 40% reported new physical illnesses (e.g., aches and pains, heart palpitations, sweating, stomach issues); and
- 23% reported a start or relapse into unhealthy or addictive behaviors.[48]

82. Annual monetary losses from identity theft are well into the billions of dollars. According to a 2007 FTC report on identity theft:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft—for example, health-related or criminal record fraud—face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[49]

---

[47] IDENTITY THEFT RES. CTR., *2022 Consumer Impact Report*, https://www.idtheftcenter.org/wp-content/uploads/2023/03/2022-Consumer-Impact-Report_V4.1_2023-Update.pdf (last visited Sept. 28, 2023).
[48] *Id.*
[49] FTC, The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* (Apr. 2007), at 11, https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Sept. 28, 2023).

83. The unauthorized disclosure of Social Security numbers can be particularly damaging because they cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been incurred. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other personal information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[50]

84. The unauthorized disclosure of sensitive personal identifying information to data thieves also reduces the value to its owner, which has been recognized by courts as an independent form of harm.[51]

85. And consumers are injured every time their data is stolen and placed on the dark web—even if they have been victims of previous data breaches. Indeed, the dark web comprises multiple discrete repositories of stolen information that can be aggregated or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases

---

[50] SOCIAL SECURITY ADMINISTRATION, *Identity Theft and Your Social Security Number* (July 2021), at 6, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Sept. 28, 2023).

[51] *See, e.g., In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp.3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

the likelihood that a victim's personal information will be exposed to more individuals who are seeking to misuse it at the victim's expense, thereby fostering an ongoing, and potentially exponential, form of injury.

86. Because of the Data Breach, Plaintiffs and Class members have suffered, and will continue to suffer, economic loss and actual non-economic harms for which they are entitled to damages, including, but not limited to, the following:

a. invasion of privacy via the non-consensual disclosure of confidential information to third parties;

b. diminished value of the PII;

c. the value of the unauthorized access of the PII;

d. diminished value of explicit and implicit promises of data security;

e. costs of fraud related to the theft of the PII;

f. costs, both realized and ongoing, associated with the detection and prevention of identity theft;

g. unauthorized use of financial accounts and costs related thereto;

h. anxiety, emotional distress, and loss of privacy, both realized and ongoing;

i. diminished credit scores resulting from credit inquiries following fraudulent activities; and

j. costs associated with time spent, lost productivity, stress, and reduced enjoyment of life because of the need to identify, monitor, and mitigate realized and likely future consequences of the Data Breach.

87. Even in instances where an individual is reimbursed for a financial loss due to identity theft or related fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. Likewise,

the DOJ's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" caused by identity theft or associated fraud.[52]

88. There may also be a significant lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches: "law enforcement officials told us that, in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[53]

89. Plaintiffs and Class members seek to recover the value of the unauthorized access to the PII permitted by ULX's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret-protected technology.

90. Nevertheless, a plaintiff may generally recover the reasonable-use value of such intellectual property—i.e., a "reasonable royalty"—from an infringer. This is true even though an infringer's use did not interfere with the owner's own use (as in the case of a nonpracticing

[52] U.S. DEP'T OF JUSTICE, Office of Justice Programs, Bureau of Justice Statistics, Erika Harrell, "Victims of Identity Theft, 2014" (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 28, 2023).
[53] U.S. GOV'T ACCOUNTABILITY OFF., Report to Congressional Requesters: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Sept. 28, 2023).

patentee) and even though the owner would not have otherwise licensed such intellectual property to an infringer.

91. A similar royalty or license measure of damages is appropriate here under common-law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class members have a protectible property interest in the PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) that rental value is established with reference to market value—i.e., based on evidence as to the value of similar transactions.

92. ULX's delayed notice also caused Plaintiffs and Class members harm. By waiting four or more months to disclose the Data Breach and by downplaying the risk of misuse, ULX prevented victims from taking meaningful, proactive, and targeted mitigation measures to secure the PII.

93. Although ULX offered some Plaintiffs and Class members the option to activate credit-monitoring services, credit monitoring is reactionary and cannot mitigate the "risk of identity theft" because it is not a preventative tool.

94. Instead, credit monitoring can alert someone to identity theft or fraud *after it has already occurred* so that, hopefully, the harm can be mitigated. Additionally, twenty-four months of credit monitoring is inadequate as victims will need to monitor their credit profiles for identity theft and fraud indefinitely given the nature of the information stolen.

95. As a result of ULX's failure to protect the PII with which it was entrusted, Plaintiffs and Class members have been placed at an imminent and ongoing risk of harm from identity theft and identity fraud, requiring them to spend time and money to mitigate the actual and potential impact of the Data Breach.

96. Such efforts include, but are not limited to, initiating "freezes" and "alerts" with credit-reporting agencies, contacting financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring financial accounts and credit reports for unauthorized activity.

97. Further, ULX continues to hold Plaintiffs' and Class members' PII and, therefore, they have an interest in ensuring that the PII is secured and not subject to further theft.

ALLEGATIONS RELATING TO PLAINTIFFS

Plaintiff Jeremy Krant

98. Plaintiff Krant was hired by ULX in July 2020 and served as Vice President of Business Development.

99. As a condition of his employment, Plaintiff Kratt provided ULX with significant amounts of his personal and financial information, including his name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information.

100. Plaintiff Krant left ULX in August of 2022 to pursue another opportunity.

101. In late April 2023, Plaintiff Krant received a letter from the IRS stating that someone had attempted to fraudulently file his taxes.

102. Plaintiff Krant reached out to Defendant about the fraudulent activity and, on May 8, 2023, received the below email from general counsel Eric Kelly that read, in part:

Dear Jeremy,

Thank you for informing us of the notice you received from the IRS.

We have reason to believe that a portion of our HR data was compromised during the security incident that occurred in March, and we are working with a third-party partner to review all of the files that were potentially in scope. We are also working with legal counsel to ensure that UnitedLex complies with all notice requirements for individuals impacted by the security incident. That said, we cannot presently identify the security incident as the reason for the IRS notice you received, but we certainly appreciate the suspicious timing and your concern. We share those concerns.

While this investigation and review is ongoing, we highly recommend that you continue to keep an eye out for other suspicious activity involving your personal information or that of other current or former UnitedLex employees. That activity may be in the form of e-mails, texts, calls, or other means. If you receive a call, please pay close attention to the caller's number, information provided or demanded, and the caller's accent – as requested by the FBI, to whom we reported the security incident in early March. We are continuing to provide the FBI with information as it becomes available.

103. Mr. Krant later received a letter in the mail from ULX, dated July 11, 2023, thereby notifying him of the breach four months after he first experienced identity theft and fraud.

104. As a result of the Data Breach, Plaintiff Krant has expended significant effort monitoring his financial accounts for potential fraudulent activity. He also had to initiate a credit freeze, which can make purchasing items on credit time-consuming and difficult.

105. In addition to spending time, money, and effort because of the Data Breach, Plaintiff Krant has suffered stress and anxiety worrying about his safety and financial well-being.

106. Given the highly sensitive nature of the information stolen, Plaintiff Krant remains at a substantial and imminent risk of future harm.

Plaintiff Todd Deaton

107. Plaintiff Deaton started the United States division of ULX in 2007, with founder Dave Deppe. Plaintiff Deaton left ULX in 2015 and returned in 2017, where he worked in sales.

108. As a condition of his employment, Plaintiff Deaton provided ULX with significant amounts of his personal and financial information, including his name and address, Social Security

number, bank and financial account information, insurance information, and payroll and tax information.

109. Plaintiff Deaton first heard rumors of the Data Breach in early 2023 while working at ULX. He was told by ULX management that the Data Breach was a non-issue and was directed to relay similar sentiments to ULX's clients.

110. By May 2023, Plaintiff Deaton no longer felt comfortable with what he was being told to tell clients about the Data Breach and this contributed to his decision to leave ULX to work for a competitor.

111. Plaintiff Deaton later received a letter from ULX, dated July 11, 2023, notifying him about the breach.

112. On July 17, 2023, Plaintiff Deaton received a letter from Merrill/Bank of America stating that someone applied for a self-directing investing account using his information and listed a mailing address in Newark, New Jersey, where Plaintiff Deaton had no connection.

113. As a result of the Data Breach, Plaintiff Deaton spent significant time and effort to address the attempted identity theft and fraud and now must continuously monitor his financial accounts for potential fraudulent activity.

114. In addition to spending time, money, and effort as a result of the Data Breach, Plaintiff Deaton has suffered stress and anxiety worrying about his safety and financial well-being.

115. Given the highly sensitive nature of the information stolen, Plaintiff Deaton remains at a substantial and imminent risk of future harm.

Plaintiff Thomas Nash

116. Plaintiff Nash was hired by ULX in July 2019, after working for LeClair Ryan. He served as marketing coordinator for ULX until approximately December 2020.

117. As a condition of his employment, Plaintiff Nash provided ULX with significant amounts of his personal and financial information, including his name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information. He also provided names and Social Security numbers for his wife and minor child.

118. During spring 2023, Plaintiff Nash fell victim to tax fraud. While doing his taxes on TurboTax, he tried to e-file and was told someone had already filed a return on his behalf.

119. Plaintiff Nash had to apply for a PIN with the IRS and confirm his identity was stolen. He had to spend significant time and effort addressing the fraud, including paying extra to mail his tax returns and losing the value of his TurboTax purchase.

120. On approximately February 23, 2023, Plaintiff Nash received an alert from his Chase credit card, which flagged that a new line of credit had been opened by someone with an unrecognized address in Queens, New York.

121. Plaintiff Nash later received a letter from ULX, dated July 11, 2023, notifying him of the Data Breach.

122. As a result of the Data Breach, Plaintiff Nash has spent significant time and effort addressing the attempted identity theft and fraud and now must continuously monitor his financial accounts for potential fraudulent activity. He also had to initiate a credit freeze, which can make purchasing items on credit time consuming and difficult.

123. In addition to spending time, money, and effort as a result of the Data Breach, Plaintiff Nash has suffered stress and anxiety worrying about the safety and financial well-being of himself and his family.

124. Given the highly sensitive nature of the information stolen, Plaintiff Nash remains at a substantial and imminent risk of future harm.

Plaintiff Shana Vachhani

125. Plaintiff Shana Vachhani's husband, Neil, worked for ULX from 2020-21, in the e-discovery department.

126. Plaintiff Vachhani's name and Social Security number were given to ULX when she was listed as a beneficiary to her husband's 401k and health insurance.

127. In approximately April 2023, Plaintiff Vachhani attempted to file her 2022 taxes with Turbo Tax, but her submission was rejected because someone had already filed taxes listing her as a dependent.

128. Plaintiff Vachhani had to report this fraud to the IRS and work with the IRS to confirm her identity, which was an extensive and time-consuming process.

129. Plaintiff Vachhani's husband later received a letter from ULX, dated July 11, 2023, notifying him of the Data Breach and alerting him that, if he had provided ULX with the names and Social Security numbers of dependents, this information may also have been affected.

130. Plaintiff Vachhani did not receive a notice about the Data Breach from ULX.

131. Plaintiff Vachhani's husband was offered free credit monitoring, but this offer was not extended to Plaintiff Vachhani, even though the letter specifically stated dependents may have been impacted by the Data Breach.

132. As a result of the Data Breach, Plaintiff Vachhani spent significant time and effort addressing the tax fraud including working extensively with the IRS to confirm her identity.

133. In addition to spending time, money, and effort as a result of the Data Breach, Plaintiff Vachhani has suffered stress and anxiety worrying about the safety and financial well-being of herself and her family.

134. Given the highly sensitive nature of the information stolen, Plaintiff Vachhani remains at a substantial and imminent risk of future harm.

Plaintiff Kimberly Miller

135. Plaintiff Kimberly Miller was hired by ULX in August of 2020.

136. As a condition of her employment, Plaintiff provided ULX with significant amounts of her personal and financial information, including her name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information.

137. Plaintiff Kimberly Miller left ULX in May of 2022.

138. In April of 2023, Plaintiff Kimberly Miller was a victim of tax fraud. When her tax advisor went to file her taxes, there was a message that it was not possible because someone had already filed a tax return using her name and social security number.

139. Plaintiff Kimberly Miller had never been the victim of identity theft or tax fraud before, and had to apply for a PIN with the IRS to confirm her identity was stolen; this took a significant amount of time and effort.

140. Plaintiff later received a letter from ULX dated July 11, 2023, notifying her about the breach.

141. Plaintiff Kimberly Miller has expended significant effort monitoring her financial accounts for potential fraudulent activity after being informed of the Data Breach. She also had

to initiate a credit freeze, which can make purchasing items on credit time-consuming and difficult.

142. In addition to spending time, money, and effort as a result of the Data Breach, Plaintiff Kimberly Miller has suffered stress and anxiety worrying about the safety and financial well-being of herself and her family.

143. Given the highly sensitive nature of the information stolen, Plaintiff Kimberly Miller remains at a substantial and imminent risk of future harm.

CLASS ACTION ALLEGATIONS

144. Plaintiffs seek relief individually and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and/or (c)(4), Plaintiffs seek certification of a nationwide class defined as follows:

> **All persons whose PII was compromised as a result of the Data Breach announced by ULX on or about March 6, 2023 (the "Class").**

145. Plaintiff Krant, as a California resident at all relevant times, seeks relief individually and as a representative of all persons who meet the following definition:

> **All persons whose PII was compromised as a result of the Data Breach announced by ULX on or about March 6, 2023, and who were California residents at the time of the Data Breach (the "California Sub-Class").**

146. Plaintiff Nash, as a Virginia resident at all relevant times, seeks relief individually and as a representative of all persons who meet the following definition:

> **All persons whose PII was compromised as a result of the Data Breach announced by ULX on or about March 6, 2023, and who were Virginia residents at the time of the Data Breach (the "Virginia Sub-Class").**

147. Plaintiffs reserve the right to amend the foregoing definitions and/or to define further sub-classes before this Court determines whether class certification is appropriate.

148. Excluded from the Class are Defendant, any entity in which ULX has a controlling interest, ULX's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

149. **Ascertainability**. The members of the Class are readily identifiable and ascertainable. ULX possesses the information needed to identify and contact Class members.

150. **Numerosity** (Fed. R. Civ. P. 23(a)(1)). Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, preliminary information suggests there are thousands of individuals whose PII was compromised in the Data Breach.

151. **Commonality** (Fed. R. Civ. P. 23(a)(2) and (b)(3)). Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. These common questions include, but are not limited to:

a. Whether Defendant knew, or should have known, of the susceptibility of its systems to a data breach;

b. Whether Defendant failed to implement reasonable and adequate security procedures and practices;

c. Whether Defendant's security measures to protect its systems were reasonable in light of known legal requirements;

d. Whether Defendant took adequate measures to protect Plaintiffs and Class members' PII after evidence of unauthorized access on its network was discovered;

e. Whether Defendant owed a duty to Plaintiffs and Class members to protect the PII;

f. Whether Defendant breached its duty to protect the PII of Plaintiffs and Class members by failing to provide adequate data security;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems and/or the loss of the PII;

h. Whether Defendant had a contractual obligation to use reasonable security measures and whether it complied with such contractual obligations;

i. Whether, as a result of Defendant's conduct, Plaintiffs and Class members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

j. Whether, as a result of Defendant's conduct, Plaintiffs and Class members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

152. **Typicality** (Fed. R. Civ. P. 23(a)(3)). Plaintiffs' claims are typical of the Class members' claims. The rights of Plaintiffs and the other Class members were violated in a virtually identical manner as a direct and/or proximate result of ULX's willful, reckless and/or negligent actions and/or inaction as to the data breach(es). Further, all such claims:

a. Present the same elements and burden of proof;

b. Rely upon Defendant's same course of conduct;

c. Rely upon the same legal arguments; and

d. Rely upon the same methods to measure damages.

153. **Adequacy** (Fed. R. Civ. P. 23(a)(4)). Plaintiffs and the undersigned counsel are adequate to represent the Class. Plaintiffs will fairly and adequately protect the interests of the Class and Plaintiffs' counsel are qualified, experienced class-action lawyers who are able to devote the time and resources necessary to represent Plaintiffs and the Class.

154. **Superiority (**Fed. R. Civ. P. 23(b)(3)). Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy. Further, no unusual difficulties are likely to be encountered in the management of this class action.

The primary purpose of the class-action mechanism is to permit litigation against wrongdoers when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant and, thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Similarly, individual litigation by each Class member would strain the court system. Individual litigation would also foster the potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class-action structure presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

155. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

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

a. Whether Defendant owed a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, and safeguarding the PII;

b. Whether Defendant failed to take reasonable steps to safeguard the PII; and

Whether Defendant failed to adequately monitor and audit its data-security systems.

COUNT I
Negligence
(*On Behalf of Plaintiffs and the Class*)

157. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

158. Defendant owed a duty to Plaintiffs and the Class members to safeguard and protect the PII.

159. That duty of care arose from Defendant's retention of 'Plaintiffs and the Class members' sensitive personal identifying information incident to its employment of Plaintiffs and the Class members as employees, independent contractors, and/or clients.

160. Defendant breached its duty by failing to exercise reasonable care in safeguarding Plaintiffs and the Class members' PII.

161. ULX also owed Plaintiffs and the Class members a duty of care to inform them of the Data Breach and attendant risks associated with the breach within a reasonable amount of time of ascertaining the same.

162. It was reasonably foreseeable that ULX's failure to exercise reasonable care in safeguarding Plaintiffs and the Class members' PII would result in an unauthorized party gaining access to such information without a lawful purpose.

163. It was reasonably foreseeable that ULX's failure to exercise reasonable care in notifying Plaintiffs and the Class members as to the theft of the PII would handicap their ability to mitigate damages from that theft.

164. As a direct and proximate result of ULX's conduct, Plaintiffs and the Class members have suffered, and will continue to suffer, damages including, but not limited to: (i) the unconsented lost value of the PII and loss of control over the same; (ii) non-consensual

publication and/or theft of the PII; (iii) out-of-pocket expenses associated with the prevention, detection, and mitigation of injuries from identity theft, tax fraud, and/or unauthorized use of the PII; (iv) costs related to addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports or accounts; (vi) anxiety, emotional distress, loss of privacy, and other non-economic injuries; (vii) ongoing risk to the PII, which remains in ULX's possession and is subject to further unauthorized disclosures so long as ULX fails to undertake appropriate and adequate measures to protect it; (viii) the cost of ongoing credit monitoring and identity-protection services necessitated by the Data Breach; (ix) compensation for the reasonable-use value of the PII; and (x) any nominal damages as deemed appropriate.

COUNT II
Negligence *Per Se*
(*On Behalf of Plaintiffs and the Class*)

165. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

166. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as ULX, of failing to use reasonable measures to protect PII. *See* 15 U.S.C. § 45(a)(1).

167. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs and the Class members' PII and by failing to comply with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature of the PII it obtained and stored.

168. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

169. Plaintiffs and the Class members are within the class of persons that the FTC Act was intended to protect.

170. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures, caused the same type of harm as that suffered by Plaintiffs and the Class.

171. As a direct and proximate result of ULX's negligence *per se*, Plaintiffs and the Class members have suffered, and will continue to suffer, injuries, damages, and harm as described herein.

COUNT III
Breach of Implied Contract
(*On Behalf of Plaintiffs and the Class*)

172. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

173. As a condition of their employment or relationship, Plaintiffs and the Class members were required to provide the PII to ULX.

174. Implicit in the agreement between ULX and Plaintiffs and the Class members was Defendant's obligation to implement and maintain reasonable safeguards in compliance with industry-standard data security practices and to protect the PII.

175. Additionally, ULX implicitly promised and agreed to retain the PII only under the condition that such information be kept secure and confidential, and only as long as reasonably necessary to perform essential business functions. As such, ULX had a duty to reasonably safeguard and protect the PII of Plaintiffs and the Class members from unauthorized disclosure or access.

176. Defendant breached its implied agreement with Plaintiffs and the Class members by failing to take appropriate measures to protect the confidentiality and security of the PII, resulting in the Data Breach.

177. As a direct and proximate result of ULX's breach, Plaintiffs and the Class members suffered injury and sustained actual losses and damages, as described herein. Plaintiffs and the Class members alternatively seek an award of nominal damages.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Class)

178. Plaintiffs incorporate here by reference all previous paragraphs, as though fully set forth herein.

179. Plaintiffs and the Class members maintained a confidential relationship with ULX whereby Defendant assumed a duty to not disclose the PII to unauthorized third parties. The PII was confidential, novel, highly personal, and sensitive.

180. ULX knew Plaintiffs and the Class members' PII was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreed to protect the confidentiality and security of the PII it collected, stored, and maintained.

181. The Data Breach comprised unauthorized disclosure of Plaintiffs and the Class members' PII, in violation of this understanding. This non-consensual disclosure occurred because ULX failed to implement and maintain reasonable safeguards to protect the PII in its possession. ULX's recklessness in failing to comply with industry-standard data security practices amounts amounted to intentional behavior.

182. Plaintiffs and the Class members suffered harm the moment the unauthorized disclosure of the PII to a third party occurred.

183. As a direct and proximate result of ULX's breach of confidence, Plaintiffs and the Class members suffered injury and sustained actual losses and damages, as alleged herein. Plaintiffs and the Class members alternatively seek an award of nominal damages.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

184. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

185. A fiduciary relationship existed between ULX and Plaintiffs and the Class members. Plaintiffs and the Class members placed Defendant in a position of trust and confidence by providing it with the PII as a condition of their employment or otherwise relationship, which PII was accepted and appreciated by ULX.

186. Defendant assumed a duty not to disclose the PII provided by Plaintiffs and the Class members to unauthorized third parties. Again, the PII was confidential, novel, highly personal, and sensitive.

187. ULX breached the fiduciary duty owed to Plaintiffs and the Class members by failing to act with the utmost good faith, fairness, and honesty, and failing to protect the PII in its possession.

188. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiffs and the Class members suffered injury and sustained actual losses and damages, as described herein. Plaintiffs and the Class members alternatively seek an award of nominal damages.

COUNT VI
Fraudulent Concealment
(*On Behalf of Plaintiffs and the Class*)

189. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

190. ULX had knowledge of the Data Breach by March 6, 2023, including the knowledge that Plaintiffs and the Class members were at significant risk of identity theft and related fraud, which they could not otherwise have known or discovered through the existence of reasonable diligence.

191. Defendant had legal and equitable duties to disclose the Data Breach to Plaintiffs and the Class members within a reasonable timeframe after it learned, or should have known, of the breach.

192. ULX deliberately failed to communicate this information to Plaintiffs and the Class members, attempting to conceal the existence of the Data Breach and attendant risks of harm associated with it.

193. Plaintiffs and the Class members justifiably relied on ULX to communicate the existence of the Data Breach and attendant risks of harm associated with it.

194. Plaintiffs and the Class members were injured by ULX's failure to communicate this information as they were unable to take actions to prevent and/or mitigate the harms of identity theft and related fraud before they occurred.

195. As a direct and proximate result of Defendant's fraudulent concealment, Plaintiffs and the Class members suffered injury and sustained actual losses and damages, as described herein. Plaintiffs and class members alternatively seek an award of nominal damages.

COUNT VII
Declaratory Judgment
(*On Behalf of Plaintiffs and the Class*)

196. Plaintiffs incorporate here by reference all previous paragraphs as though fully set forth herein.

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

198. An actual controversy has arisen in the wake of the Data Breach given ULX's present and prospective duties under the common law, and other sources of law, to reasonably safeguard the PII.

199. Defendant's misconduct, as described herein, gives rise to a genuine question as to whether it is currently maintaining data-security measures adequate to protect Plaintiffs and the Class members from further cyberattacks that could compromise their PII.

200. Defendant still possesses the PII, which means it remains at risk of further breach because Defendant's data-security measures remain inadequate. Plaintiffs and the Class members continue to suffer injuries as a result of the theft of their PII and remain at an imminent risk that further such compromises will occur in the future.

201. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) ULX's existing data-security measures do not satisfy its obligations and duties of care; and (b) in order to comply with its obligations and duties of care, ULX must: (i) purge, delete, or destroy, in a reasonably secure manner, Plaintiffs' and the Class members' PII if the PII is no longer necessary

to perform essential business functions, so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engagement of third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing, including simulated attacks, penetration tests, and audits of ULX's systems on a periodic basis, and ordering ULX to promptly correct any problems or issues detected by such third-party security auditors;

b. engagement of third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training of Defendant's security personnel regarding any new or modified procedures;

d. encryption and segmentation of the PII by, amongst other things, the creation of firewalls and access controls such that, if one area of ULX's system is compromised, hackers cannot gain access to other portions of the system;

e. purging, deleting, and destroying, in a reasonable and secure manner, PII not necessary to perform essential business functions;

f. conducting regular database scans and security checks;

g. conducting regular employee education regarding best security practices;

h. implementation of multi-factor authentication and POLP to combat system-wide cyberattacks; and

i. conducting routine, continuous internal training and education to inform internal security personnel how to identify, manage, and contain a breach.

COUNT VIII
Violation of the California Constitution's Right to Privacy, Cal. Const. Art. I, § 1
(*On Behalf of Plaintiff Krant and the California Sub-Class*)

202. Plaintiff Krant, individually and on behalf of the California Sub-Class, incorporates here by reference all previous paragraphs as though fully set forth herein.

203. The California Constitution, art. I, sect. 1, endows Plaintiff Krant and the California Sub-Class with inviolate rights, including the protection of the members' privacy.

204. This comprises a legally cognizable interest in not having private information misused or improperly disseminated.

205. Plaintiff Krant and the members of the California Sub-Class reasonably expected that Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal and financial information.

206. As described, besides holding itself out as an expert in data security and legal compliance in such regard, ULX apparently engaged in negotiations with the hackers and, for reasons that aren't rationally ascertainable, refused to pay what was, in context, a modest ransom; declined to utilize insurance to pay the ransom despite presumably carrying significant cybercrime coverage; and, in so doing, not only abetted the release of a significant amount of private information but, thereafter, procrastinated in notifying impacted parties while also lying about the same. As a result, Plaintiff Krant and the members of the California Sub-Class will have their private information for sale on the dark web indefinitely.

207. Defendant's conduct resulted in a serious invasion of the privacy of Plaintiff Krant and the members of the California Subclass, as the release of personal and financial information, including but not limited to Social Security numbers, dates of birth, cell-phone numbers, and bank account numbers, could highly offend a reasonable individual.

208. As a direct consequence of the actions identified above, Plaintiff Krant and the members of the California Sub-Class suffered harms and losses including, but not limited to, economic loss, the loss of control over the use of their identities, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to remedy harm to their privacy, the need to dedicate future time and expenses remediation and prevention of further loss, and privacy injuries caused by having their personal and financial information disseminated.

COUNT IX
Violation of Virginia Data Breach Notification Law,
Va. Code. Ann. §§ 18.2-186.6, *et seq.*
(*On Behalf of Plaintiff Nash and the Virginia Sub-Class*)

209. Plaintiff Nash, individually and on behalf of the Virginia Sub-Class, incorporates here by reference all previous paragraphs as though fully set forth herein.

210. ULX was, and is, required to accurately notify Plaintiff Nash and Virginia Sub-Class members following discovery or notification of a breach of its data if unencrypted or unredacted PII was/is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

211. Defendant is an entity that owns or licenses computerized data that includes "personal information" as defined by Va. Code Ann. § 18.2-186.6(B).

212. Plaintiff Nash and Virginia Sub-Class members' PII includes "personal information" covered by Va. Code Ann. § 18.2-186.6(A).

213. Because ULX discovered a breach of its security system in which unencrypted or unredacted "personal information" was reasonably believed to have been accessed and acquired by an unauthorized person, who would, or was reasonably believed would, engage in identify theft or other fraud, it had an obligation to disclose the data breach in a timely and accurate fashion, as mandated by Va. Code Ann. § 18.2-186.6(B).

214. By failing to disclose the Data Breach in a timely and accurate manner, ULX violated Va. Code Ann. § 18.2-186.6(B).

215. As a direct and proximate result of ULX's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff Nash and Virginia Sub-Class members were unable to take actions to prevent and/or mitigate the harms of identity theft and related fraud, as described above.

216. Plaintiff Nash and Virginia Sub-Class members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

PRAYER FOR RELIEF

217. WHEREFORE, Plaintiffs, individually and on behalf of members of the Class and sub-classes, as applicable, respectfully request the Court enter judgment in their favor and against Defendant in the form of:

a. An order certifying the Class and sub-classes, as defined herein, and appointing Plaintiffs as Class representatives and appointing the undersigned counsel as lead counsel for the Class;

b. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and the Class members' PII;

c. Equitable relief compelling Defendant to use industry-standard security methods and policies with respect to data collection, storage and protection, and sharing of information, and to dispose of Plaintiffs and the Class members' that is not necessary to perform essential business functions;

d. An award of compensatory, consequential, and general damages in an amount to be determined at trial;

e. An award of statutory, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

f. An award of attorneys' fees, costs, and litigation expenses, as allowable by law;

g. Pre-judgment interest on all amounts awarded; and

h. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiffs demand a jury trial on all claims so triable.

DESIGNATION OF PLACE OF JURY TRIAL

Plaintiffs designate Kansas City, Kansas as the place for this case to be tried to a jury.

Dated: September 29, 2023

Respectfully submitted,

/s/ *Norman E. Siegel*
Norman E. Siegel (D. Kan. No. 70354)
J. Austin Moore (D. Kan. No. 78557)
Abby E. McClellan Paradise (D. Kan. No. 78804)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel: 816-714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com
mcclellan@stuevesiegel.com

Bryce B. Bell KS # 20866
Jenilee V. Zentrich KS # 29098
T. Grant Honnold (*to be admitted pro hac vice*)
BELL LAW, LLC
2600 Grand Blvd., Suite 580
Kansas City, Missouri 64108
Tel: 816-886-8206
Bryce@BellLawKC.com
JZ@BellLawKC.com
TGH@BellLawKC.com

Melody R. Dickson KS#24494
Tyler W. Hudson KS#20293
Eric D. Barton KS#16503
WAGSTAFF & CARTMELL
4740 Grand Avenue, Suite 300
Kansas City, MO 64112
816-701-1100
F: 816-531-2372
mdickson@wcllp.com
thudson@wcllp.com
ebarton@wcllp.cpm

Attorneys for Plaintiffs and the Proposed Classes

ClassAction.org