IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

THERESA BRYANT, individually and on behalf of all others similarly situated,	)	Case No.:
Plaintiff,	)	
v.	)	
TRANS UNION LLC,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff Theresa Bryant ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant Trans Union LLC ("Defendant" or "TransUnion"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a putative class action lawsuit based upon Defendant's widespread violations of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x ("FCRA"), arising from Defendant's failure to safeguard personally identifying information ("PII") entrusted to it in its role as a credit reporting agency, or in its role storing and transferring said information. Specifically, this action arises from Defendant's reliance on an insecure information storage and transfer system that proved readily penetrable to nefarious hackers, resulting in the exposure of

sensitive information, including but not limited to names, driver's license numbers, Social Security numbers, and financial account numbers.

2. Defendant is regulated as a consumer reporting agency ("CRA") under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681, *et seq*. Similarly, Defendant is also regulated as a consumer credit reporting agency ("CCRA") under the California Consumer Credit Reporting Agencies Act ("CCRAA"), Cal. Civ. Code §§ 1785.1, *et seq*. In fact, "TransUnion is one of the three largest credit bureaus in the world."[1] It collects, stores, and maintains a database of information from more than 1 billion individuals around the globe, including "more than 200 million files profiling nearly every credit-active consumer in the United States."[2]

3. On November 7, 2022, TransUnion reported a data breach with the Massachusetts Attorney General after information in the company's possession was subject to unauthorized access was made to its files (the "Data Breach").[3] According to TransUnion, the Data Breach resulted in the names, addresses, full Social Security numbers, financial account numbers, and complete driver's license information of certain individuals being compromised (collectively, the "PII").

4. The Data Breach affected approximately 200 million TransUnion customers in the United States.[4]

---

[1] Miles to Memories, *TransUnion Says Breach Has Exposed Consumers' Financial Information* (Nov. 11, 2022), https://www.yahoo.com/now/notice-data-breach-incident-183200387.html; *see also* https://www.creditrepairexpert.org/the-big-3-credit-reporting-agencies/.

[2] https://www.transunion.com/solution/customer-credit-check.

[3] *See* TransUnion Data Breach Notification Letter November 2022, *available at* https://www.mass.gov/doc/assigned-data-breach-number-28524-transunion-llc/download.

[4] *See* ID Strong, *TransUnion Data Breach Affects All United States Active-Credit Consumers* (Nov. 15, 2022), https://www.idstrong.com/sentinel/transunion-data-breach-affects-credit-consumers/; Techaeris, *TransUnion is the latest credit bureau to experience a data breach* (Nov. 17, 2022), https://techaeris.com/2022/11/17/transunion-is-the-latest-credit-bureau-to-experience-a-data-breach/.

5. Plaintiff received notice of the Data Breach in a letter dated November 2022.

6. Defendant owed a duty to Plaintiff and Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected and stored about them. Defendant breached said duty by failing to implement and maintain reasonable security procedures and practices to protect the PII from unauthorized access and unnecessarily using, storing, and retaining Plaintiff's and Class member's personal information on TransUnion's inadequately protected software.

7. Defendant knew that critical software was required to protect Plaintiff's and Class members' personal information.[5] Further, TransUnion prides itself on making "trust possible," and it knows that consumer trust is closely tied to, among other things, the way it safeguards and "stewards the information" it collects, stores, maintains, and/or transfers.[6] Yet, Defendant knew that the sensitive consumer information uploaded to its proprietary database was susceptible to security risks. Nonetheless, Defendant continued to store, maintain, and transmit extremely sensitive PII using this insecure software.

8. Due to Defendant's inadequate cybersecurity, Plaintiff's and Class members' PII was accessed and disclosed in the Data Breach.

---

[5] *See* TransUnion, *Data Breach Services*, https://www.transunion.com/solution/data-breach-services ("According to the ITRC, 2021 was the highest year on record for breaches – growing 23 percent over the previous all-time high. With data breaches on the rise, companies need to have plans and resources in place to be prepared, react quickly, and help resolve challenges that present themselves to their business customers, consumers, and partners. Putting an actionable program in place can preserve your business' reputation, as well as prevent the loss of customers."); *see also* TransUnion, *Data Security*, https://www.transunion.com/client-support/data-security.

[6] *About TransUnion*, https://www.transunion.com/about-us/about-transunion ("TransUnion is a global information and insights company that makes trust possible between businesses and consumers, by ensuring that each consumer is reliably represented in the marketplace. We do this by having an actionable and robust picture of each person. This picture is grounded in our foundation as a credit reporting agency which enables us to tap into both credit and public record data; our data fusion methodology that helps us link, match and tap into the awesome combined power of that data; and our knowledgeable and passionate team, who stewards the information with expertise[.]") (emphasis added); *but see* ID Strong, *TransUnion Data Breach Affects All United States Active-Credit Consumers*, *supra* ("**Unfortunately for TransUnion, there are so few people unaffected by the breach that the number of people who will fully trust the bureau is slim**.") (emphasis added).

9. Plaintiff brings this action on behalf of herself and all affected consumers whose PII was exposed as a result of the Data Breach. Plaintiff seeks, for herself and the Class, injunctive relief, actual and other economic damages, consequential damages, nominal damages or statutory damages, punitive damages, and attorney's fees, litigation expenses, and costs.

10. For the foregoing reasons, Plaintiff brings this action individually and on behalf of a Nationwide Class and California Subclass of similarly situated individuals against Defendant for: (i) violations of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681, *et seq*.; (ii) negligence; (iii) negligence *per se*; (iv) violation of California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §§ 17200, *et seq*.; (v) violation of California's Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, *et seq*.; (vi) unjust enrichment / restitution; and (vii) declaratory judgment.

JURISDICTION AND VENUE

11. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiff alleges that Defendant violated federal law, namely, the FCRA.

12. This Court has supplemental subject matter jurisdiction over Plaintiff's claims arising under state law pursuant to 28 U.S.C. § 1367(a), because Plaintiff's state law claims are so related to her FCRA claims falling within original jurisdiction "that they form part of the same case or controversy under Article III of the United States Constitution." Additionally, this Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as amended by the Class Action Fairness Act of 2005 ("CAFA"), because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are over 100 members of the putative class, and Plaintiff and most members of the proposed classes are citizens of different states than Defendant.

13. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District, and the acts and transactions giving rise to this action occurred in this District.

14. This Court is the proper venue for this action pursuant to pursuant to 28 U.S.C. § 1391 because Defendant's principal place of business is located in this District and because a substantial part of the events, omissions, and acts giving rise to Plaintiffs' claims herein occurred in this District.

THE PARTIES

15. Plaintiff Theresa Bryant is a natural person and a citizen of California who resides in Los Angeles County, California. In or about November 2022, Defendant notified Plaintiff that her PII—including, among other things, her Social Security number and email address—was accessed by unauthorized users as a result of the Data Breach. As a result of the Data Breach, Plaintiff spent time and effort investigating the Data Breach, monitoring her financial accounts, and searching for fraudulent activity. Also as a direct result of the breach, Plaintiff Sharpe spent time and money purchasing a credit freeze from Experian, in order to prevent or mitigate possible harm flowing from the Data Breach. Given the highly-sensitive nature of the information stolen, Plaintiff remains at a substantial and imminent risk of future harm.

16. Defendant Trans Union LLC ("Defendant" or "TransUnion") is a consumer reporting agency organized under Delaware law with its principal place of business located at 555 West Adams, Chicago, Illinois.

17. Plaintiff reserves the right to amend this Complaint to add different or additional defendants, including without limitation any officer, director, employee, supplier, or distributor of

Defendant who has knowingly and willfully aided, abetted, and/or conspired in the false and deceptive conduct alleged herein.

FACTUAL ALLEGATIONS

A. Background On Data Breaches

18. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so.[7]

19. Data breaches are becoming increasingly more common and harmful. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed.[8] In 2019, 3,800 data breaches were reported, with at least 4.1 billion total records exposed.[9] The average cost of a data breach in the United States in 2019 was $8.19 million.[10]

20. Consumers are harmed in a variety of ways by data breaches. First, consumers are harmed financially. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[11] However, other estimates have placed the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft—a common result of data breaches—was $298 dollars.[12] And in 2019, Javelin Strategy & Research compiled consumer complaints from the U.S. Federal Trade

[7] *See* Digital Guardian, *The History of Data Breaches* (Oct. 24, 2019), https://digitalguardian.com/blog/history-data-breaches.

[8] *See id*.

[9] *See* Norton by Symantec, *2019 Data Breaches: 4 Billion Records Breached So Far* (2019), https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html.

[10] *See* Digital Guardian, *What's the Cost of a Data Breach in 2019* (July 30, 2019), *https*://digitalguardian.com/blog/whats-cost-data-breach-2019.

[11] *See id*.

[12] *See* Norton by Symantec, *2013 Norton Report 8* (2013), https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

Commission ("FTC") and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[13]

21. Identity theft is one of the most problematic harms resulting from a data breach. With access to an individual's PII, criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name, but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[14]

22. Consumers are also harmed by the time they spend rectifying the effects of a data breach. A Presidential identity theft report from 2007 states that:

> 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, open new ones, and dispute charges with individual creditors.[15]

23. Further, the effects of a data breach on consumers are not temporary. In a report issued by the U.S. Government Accountability Office ("GAO"), the GAO found that "stolen data may be held for up to a year or more before being used to commit identity theft," and "fraudulent use of [stolen information] may continue for years" after the stolen information is posted on the

[13] *See* Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime*, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[14] *See* U.S. Federal Trade Commission, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft.

[15] U.S. Federal Trade Commission, *The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan* (Apr. 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

Internet.[16] In fact, consumers suffer 33% of the harm from a data breach after the first year.[17] Thus, consumers can lose years' worth of time dealing with a data breach.

24. The existence of these problems is not always immediately ascertainable. As the GAO Report describes:

> [L]aw 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.

25. Consumers are also harmed by the lost value of their data. Personally Identifying Information ("PII") represent important, highly valuable property rights.[18] PII can be easily commodified, allowing the information to be bought and sold.[19] This information "has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets."[20]

26. PII held by credit reporting agencies, like Defendant, is highly prized because such files contain multiple pieces of highly sensitive information, including names, addresses, telephone numbers, email addresses, and Social Security numbers, and bank account information, including

---

[16] *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (citing U.S. GOV'T ACCOUNTABILITY OFFICE, GAO–07–737, REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION (2007)).

[17] *See* Larry Ponemon, *What's New in the 2019 Cost of a Data Breach Report*, SECURITY INTELLIGENCE, https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/.

[18] *See* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[19] *See* Robert Lowes, *Stolen EHR [Electronic Health Records] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), https://www.medscape.com/viewarticle/824192.

[20] Soma, *supra*, *Corporate Privacy Trend*.

routing numbers. Such information is valued at between $1,200 to $1,300 on the black market.[21] This, according to the Federal Bureau of Investigation's ("FBI") Cyber Division, is the reason such records can be sold by criminals for roughly 50 times higher than the price of a stolen social security or credit card number on its own.[22]

27. As a result, companies have begun providing an opportunity to consumers to sell this information to advertisers and other third parties. More and more, consumers have control over who ultimately receives their PII, and when consulted, consumers place a high value on their PII as well as on the privacy of that information. Researchers have even confirmed that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

28. Thus, when consumers' PII is disclosed without their consent, consumers are deprived of both the ability to choose what is done with their information as well as the full monetary value of their information.

B. The Importance of Consumer Credit in the U.S. Economy

29. A consumer credit system allows consumers to borrow money or incur debt, and to defer repayment of that money over time. Access to credit enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.[24] Nearly all Americans rely

---

[21] Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), https://www.scmagazine.com/home/security-news/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/.

[22] Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8,2014), https://www.illuminweb.com/wp-conent/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22 INFORMATION SYSTEMS RESEARCH 254, 254 (2011), https://www.jstor.org/stable/23015560?seq=1#page_scan_tab_contents.

[24] *See* U.S. Federal Trade Commission, *Consumer Credit Law & Practice in the U.S.*, https://www.ftc.gov/sites/default/files/attachments/training-materials/law_practice.pdf.

on credit to make everyday purchases using credit cards, obtain student loans and further education, gain approval for items like cellular phones and Internet access, and to make major life purchases such as automobiles and homes.

30. In order for this system of credit to be efficient and effective, a system of evaluating the credit of consumers is required. The earliest American systems of credit evaluation were retailers relying on personal reputation and standing in the community to determine creditworthiness. U.S. credit reporting agencies started as associations of retailers who shared their customers' credit information with each other including those deemed as credit risks.[25]

31. As the nation grew after World War II, and banks and finance companies took over from retailers as the primary source of consumer credit, a more quantitative and objective system of credit rating emerged. The development of computers, which could store and process large amounts of data, enabled the CRAs to efficiently collect and provide credit information to consumer lenders on a national basis.[26]

32. Today, creditors such as banks and mortgage companies loan money to consumers, track the consumers' payment history on the loan, and then provide that information to one or more CRAs. The CRAs track all of the payment history they receive relating to a single consumer and compile that information as part of a consumer's credit reporting "file."[27]

33. A consumer's credit reporting file contains identifying information such as the consumer's name, date of birth, address, and Social Security Number (SSN), as well as payment information on past credit accounts, including the name of the lender, the original amount of the loan, the type of the loan, and how much money the consumer still owes on that loan. A consumer

[25] *See id*.

[26] *See id*. at 2.

[27] *Id*.

file also contains details on the consumer's payment history on past credit accounts—which helps potential lenders estimate how likely the consumer is to pay back the full amount of a loan on time—and information in the public record which might affect the consumer's ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or information relating to tax liabilities.[28]

34. Because consumers have little or no control over the information that CRAs gather and store, the accuracy and security of the information they compile is at the heart of a fair and accurate credit reporting system. Information that is inaccurate can lead to uninformed credit decisions, and information that is unsecure can lead to identify theft, fraud, and widespread distrust of CRAs—with systemic consequences for the entire national economy.

C. TransUnion Compiles Massive Amounts of Consumer Information

35. Over the last several decades, TransUnion expanded rapidly by acquiring numerous companies and increasing its data collection capacity. By the late 1990s, industry consolidation resulted in three major CRAs controlling the market: TransUnion, Equifax, and Experian.

36. TransUnion's business model involves aggregating data relating to consumers from various sources, compiling that data in a usable format known as a credit report, and selling access to those reports to lenders interested in making credit decisions, financial companies, employers, and other entities that use those reports to make decisions about individuals in a range of areas.[29] Because the extension of credit relies on access to consumers' credit files, the CRAs have been

[28] *See id*. at 1.

[29] *See, e.g.*, https://www.transunion.com/business ("We help businesses find their best customers and determine the right ways to serve and keep them - through access to products and services that help them achieve their goals."); https://www.transunion.com/solution/multi-family-data-reseller.

referred to as the "linchpin[s]" of the U.S. financial system.[30] TransUnion also sells information directly to consumers, including access to their own credit file.[31] Based on these products and services, TransUnion's business generated $2.96 billion in annual revenues for 2021, a 16.98% increase from 2020.[32]

37. TransUnion recognizes that the value of its company is inextricably tied to its massive trove of consumer data.[33] For that reason, TransUnion has aggressively acquired companies with the goal of expanding into new markets and acquiring proprietary data sources.[34]

38. For example, in 2018, TransUnion acquired Callcredit Information Group, Ltd., another consumer credit bureau and information solutions company that, like TransUnion, provides data, analytics, and technology solutions to help businesses and consumers make

---

[30] The Wall Street Journal, *'We've Been Breached': Inside the Equifax Hack* (Sep. 18, 2017), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318.

[31] *See* https://www.transunion.com/?atvy=%7B%22191010%22%3A%22Experience+A%22%7D; https://www.transunion.com/customer-support/contact-us-consumers.

[32] See Macro Trends, *TransUnion Revenue 2011-2022*, https://www.macrotrends.net/stocks/charts/TRU/transunion/revenue.

[33] *See* TransUnion Q3 2022 Form-10-Q, at 33, *available at* https://investors.transunion.com/~/media/Files/T/Transunion-IR/reports-and-presentations/transunion-q3-2022-form-10-Q.pdf ("**Grounded in our heritage as a credit reporting agency, we have built robust and accurate databases of information for a large portion of the adult population in the markets we serve**. We use our data fusion methodology to link and match an increasing set of disparate data to further enrich our database. … **Leveraging our established position as a leading provider of information and insights, we have grown our business by expanding the breadth and depth of our data**[.] … As a result, over the long term we believe we are well positioned to expand our share within the markets we currently serve and capitalize on the larger data and analytics opportunity. Our solutions are based on a foundation of data assets across financial, credit, alternative credit, identity, phone activity, digital device information, marketing, bankruptcy, lien, judgment, insurance claims, automotive and other relevant information obtained from thousands of sources including financial institutions, private databases and public records repositories. **We refine, standardize and enhance this data using sophisticated algorithms to create proprietary databases**.") (emphasis added); *id*. at 34 ("We leverage our differentiated capabilities in order to serve a global customer base across multiple geographies and industry verticals. … We have been successful in leveraging our brand, our expertise and our solutions and have a leading presence in several high-growth international markets. Millions of consumers across the globe also use our data to help manage their personal finances and take precautions against identity theft.") (emphasis added).

[34] *See id*. at 12-14, 35-36, 41; *see also* Mergr, *TransUnion Mergers and Acquisitions Summary*, https://mergr.com/transunion-holding-acquisitions ("TransUnion has acquired 20 companies, including 13 in the last 5 years. … The Company's most targeted sectors include information technology (56%) and software (12%).").

informed decisions, for $1.4 billion.[35] In 2021, TransUnion also acquired Neustar, which is "an information services and technology company and a leader in identity resolution providing … data on people, devices, and locations, continuously corroborated through billions of transactions" that "serves more than 8,000 clients worldwide, including 60 of the Fortune 100."[36] The sale closed at $3.1 billion, making this TransUnion's "largest acquisition to date."[37] On the same day, TransUnion also announced its acquisition of Sontiq,[38] upon which TransUnion gained access to Sontiq's database of information relating to its more than 770,000 business customers, which includes information regarding more than 49 million individuals. Most recently, in April of 2022, TransUnion announced its acquisition of "Verisk Financial Services ('Verisk Financial'), the financial services business unit of Verisk (Nasdaq: VRSK), for $515 million."[39]

39. TransUnion now maintains information on 1 billion individuals worldwide, including over 200 million individual consumers in the United States alone.

---

[35] TransUnion Newsroom, *TransUnion Completes Acquisition of Callcredit* (Jun. 19, 2018), https://newsroom.transunion.com/transunion-completes-acquisition-of-callcredit/.

[36] TransUnion Newsroom, *TransUnion and Neustar Announce Transaction Close* (Dec. 1, 2021), https://newsroom.transunion.com/transunion-and-neustar-announce-transaction-close/.

[37] TransUnion Newsroom, *TransUnion Accelerates Growth of Identity-Based Solutions with Agreement to Acquire Neustar for $3.1 Billion* (Sep. 13, 2021), https://newsroom.transunion.com/transunion-accelerates-growth-of-identity-based-solutions--with-agreement-to-acquire-neustar-for-31-billion/ ("The addition of Neustar's talent, data and products will enhance TransUnion's position as a global information and insights company providing diverse, high-growth credit and non-credit solutions at scale. … Neustar's broad customer base advances TransUnion's diversification into new markets and verticals, and presents significant opportunities for cross-selling and innovation.").

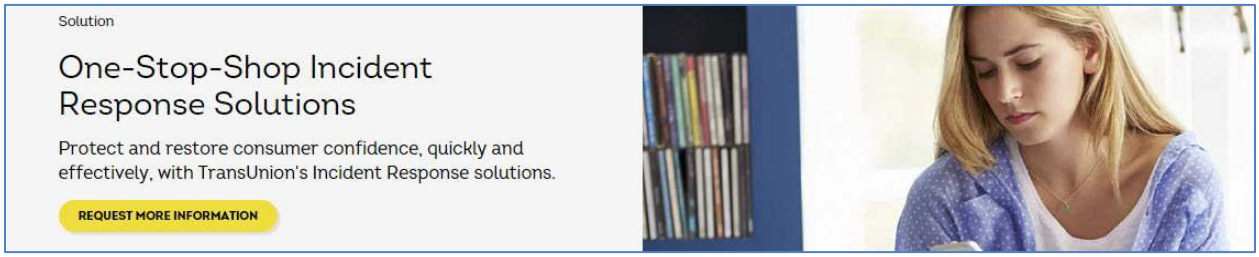
[38] *See* TransUnion Newsroom, *TransUnion Completes Acquisition of Sontiq* (Dec. 1, 2021), https://newsroom.transunion.com/transunion-completes-acquisition-of-sontiq/.

[39] TransUnion Newsroom, *TransUnion Completes Acquisition of Verisk Financial Services* (Apr. 8, 2022), https://newsroom.transunion.com/transunion-completes-acquisition-of-verisk-financial-services/ ("Verisk Financial brings to TransUnion authoritative data sets for credit and debit card accounts and demand deposit account behavior, strengthening the company's position as a leading provider of innovative solutions around the globe. … Verisk Financial[] … is relied upon by leading financial institutions, payments providers, and retailers worldwide[.]").

D. TransUnion Recognized The Importance Of Data Security

40. TransUnion was well aware of the likelihood and repercussions of cybersecurity threats, including data breaches, having observed numerous other well-publicized data breaches involving major corporations over the last decade plus, including data breaches for which it was responsible.[40] In fact, as noted above, just last year TransUnion sought to capitalize on the increase in the number of breaches during the COVID-19 pandemic by spending $638 million to acquire an identity theft protection company—Sontiq—to bolster its data breach response and product offerings.

41. As evidenced by its own product offerings, TransUnion held itself out as a leader and expert in anticipating and combatting such threats and developed and sold "data breach services"—including, *inter alia*, "TransUnion Incident Response solutions," and "Identity Restoration"— to consumers and businesses to prevent and combat the "identity theft and fraud from occurring or reoccurring."[41] TransUnion has even maintained a dedicated landing page to sell products and services specifically tailored to a data breach: https://www.transunion.com/solution/data-breach-services.



[40] See, e.g., Class Action Complaint filed in *Ramirez v. Trans Union, LLC*, Case No. 3:12-cv-00632, ECF No. 1 (N.D. Cal. Feb. 2, 2012).
[41] *See, e.g.*, TransUnion, *Data Breach Services*, https://www.transunion.com/solution/data-breach-services; TransUnion, *myTrueIdentity: Data Breach Services from TransUnion*, https://www.transunion.com/content/dam/transunion/global/business/documents/solution-data-breach-services-proactive-br-0317.pdf; TransUnion, *Data Security*, https://www.transunion.com/client-support/data-security.

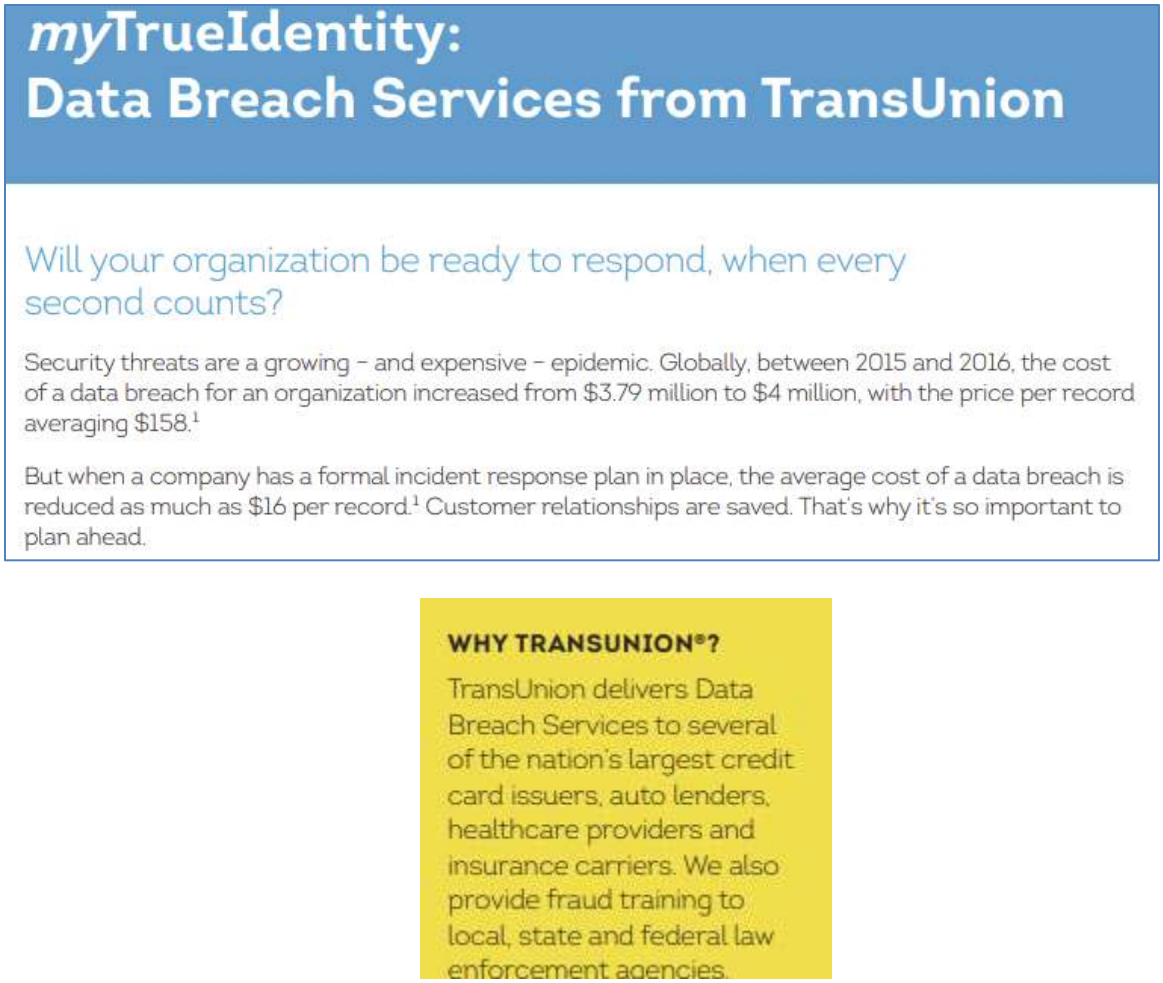
42. In its marketing materials, copied below, TransUnion acknowledges that "2021 was the highest year on record for breaches – growing 23 percent over the previous all-time high," and states: "With data breaches on the rise, companies need to have plans and resources in place to be prepared, react quickly, and help resolve challenges that present themselves to their business customers, consumers, and partners. Putting an actionable program in place can preserve your business' reputation, as well as prevent the loss of customers. The ability to notify and assist impacted individuals and get back to business as usual could make the difference between solid recovery and grinding to a halt."[42]

> Be ready for an incident before it occurs. Ease the burdens a breach can place on your brand and its consumers.
>
> According to the ITRC, 2021 was the highest year on record for breaches – growing 23 percent over the previous all-time high. With data breaches on the rise, companies need to have plans and resources in place to be prepared, react quickly, and help resolve challenges that present themselves to their business customers, consumers, and partners. Putting an actionable program in place can preserve your business' reputation, as well as prevent the loss of customers. The ability to notify and assist impacted individuals and get back to business as usual could make the difference between solid recovery and grinding to a halt.

43. In other marketing materials, TransUnion also recognizes that "Security threats are a growing – and expensive – epidemic" but that, "when a company has a formal incident response plan in place, the average cost of a data breach is reduced as much as $16 per record," which is "why it's so important to plan ahead."[43]

[42] TransUnion, *Data Breach Services*, *supra*.

[43] TransUnion, *myTrueIdentity: Data Breach Services from TransUnion*, *supra*.



44. TransUnion has also touted its "specialized team of identity restoration agents," which will "be ready to provide affected customers instant online access to the resources they'll need," including through products and services associated with "one of three packages featuring different levels of credit monitoring and identity theft protection support," in an effort to "stop the

loss of customers following a breach."[44] TransUnion also made similar representations to consumers regarding its data privacy practices.[45]

E. Defendant Collected And Stored Plaintiff's And Class Members' Personally Identifying Information, Promising To Keep It Safe

45. As noted above, Defendant collects and stores a considerable amount of consumers' PII, as is outlined on its website[46] and in its most recent Form 10-K.[47] Defendant's website and SEC filings also highlight how it uses and discloses its consumers' PII.[48]

46. Despite Defendant's representations detailed above, TransUnion knew that the sensitive personal information stored on its database was vulnerable and otherwise not secure, leaving high risk targets like Plaintiff's and the Class's PII exposed.

47. As such, Defendant was aware that PII was at high risk of theft. Accordingly, Defendant should have anticipated and taken appropriate and standard measures to protect Plaintiff's and Class member's PII against cyber-security attacks. However, TransUnion failed to do so, thereby exposing Plaintiff and Class members to the threat of data breach.

---

[44] *Id.*; *see also About TransUnion*, https://www.transunion.com/about-us/about-transunion ("TransUnion is a global information and insights company that makes trust possible between businesses and consumers, by ensuring that each consumer is reliably represented in the marketplace. We do this by having an actionable and robust picture of each person. This picture is grounded in our foundation as a credit reporting agency which enables us to tap into both credit and public record data; our data fusion methodology that helps us link, match and tap into the awesome combined power of that data; and our knowledgeable and passionate team, who stewards the information with expertise[.]") (emphasis added).

[45] *See* TransUnion, *Data Security*, https://www.transunion.com/client-support/data-security ("You can count on current credit information, because we maintain and update our database daily. Our national file includes public record information and accounts receivable data from national, regional and local credit grantors. We compile this information into a credit report that provides a consumer's payment history. To help protect the confidentiality of personal credit and payment information in our database, we follow security measures to help ensure that personal information remains private. … These and other procedures enable us to facilitate secure and unbiased transactions, which helps protect you and your customers.").

[46] *See, e.g.*, https://www.transunion.com/data-reporting/data-reporting; https://www.transunion.com/data-reporting/data-reporting-faqs.

[47] *See* TransUnion Q3 2022 Form-10-Q, at 33-34, *supra*.

[48] *See, e.g., id.*

48. Indeed, as noted above, on November 7, 2022, TransUnion reported a data breach with the Massachusetts Attorney General after information in the company's possession was subject to unauthorized access was made to its files (the "Data Breach").[49] According to TransUnion, the Data Breach resulted in the names, addresses, full Social Security numbers, financial account numbers, and complete driver's license information of certain individuals being compromised (collectively, the "PII").

49. The Data Breach affected approximately 200 million TransUnion customers in the United States.[50]

50. Plaintiff received notice of the Data Breach in a letter dated November 2022.

51. Defendant owed a duty to Plaintiff and Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard the PII it collected and stored about them. Defendant breached said duty by failing to implement and maintain reasonable security procedures and practices to protect the PII from unauthorized access and unnecessarily using, storing, and retaining Plaintiff's and Class member's personal information on TransUnion's inadequately protected software.

52. Due to Defendant's inadequate cybersecurity, Plaintiff's and Class members' PII was accessed and disclosed in the Data Breach.

53. TransUnion's failures extend to the Data Breach notice itself. For example, Defendant failed to indicate the time period of consumers' PII involved in the Data Breach. This is problematic because the "[k]ey for all services and products is to ensure file upload/sharing

[49] *See* TransUnion Data Breach Notification Letter November 2022, *available at* https://www.mass.gov/doc/assigned-data-breach-number-28524-transunion-llc/download.

[50] *See* ID Strong, *TransUnion Data Breach Affects All United States Active-Credit Consumers* (Nov. 15, 2022), https://www.idstrong.com/sentinel/transunion-data-breach-affects-credit-consumers/; Techaeris, *TransUnion is the latest credit bureau to experience a data breach* (Nov. 17, 2022), https://techaeris.com/2022/11/17/transunion-is-the-latest-credit-bureau-to-experience-a-data-breach/.

permissions are set correctly and reviewed regularly, client files are purged when no longer needed or moved to longer-term encrypted storage, and software updated on a continuous basis."[51] In other words, if the consumer PII was accessed in the Data Breach, then Defendant did not take proper steps to weed out older data from its database.

54. This information is made all the worse, considering that Defendant knew or should have known that PII is high risk targets for identity thieves.

CLASS ALLEGATIONS

55. ***Class Definition.*** Plaintiff brings this action on behalf of the following Class and Subclass:

(a) ***Nationwide Class***. Plaintiff seeks to represent a class of similarly situated individuals, defined as all persons in the United States whose PII was exposed in Defendant's November 2022 Data Breach (the "Class" or "Nationwide Class").

(b) ***California Subclass.*** Plaintiff also seeks to represent a subclass of all California residents whose PII was exposed in Defendant's November 2022 Data Breach (the "California Subclass").

56. Excluded from the Class are: (1) Defendant and its officers, directors, employees, principals, affiliated entities, controlling entities, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

[51] Mathew J. Schwartz, *Accellion Holdouts Get Legacy File Transfer Appliance Blues*, BANK INFO SECURITY (Mar. 30, 2021), https://www.bankinfosecurity.com/blogs/accellion-holdouts-get-legacy-file-transfer-appliance-blues-p-3009.

57. Plaintiff reserves the right to amend the definition of the Class and Subclass if discovery or further investigation reveals that the Class or Subclass should be expanded or otherwise modified.

58. ***Numerosity.*** Members of the Class and Subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class and Subclass number in the millions. The precise number of Class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

59. ***Commonality and Predominance.*** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Common legal and factual questions include but are not limited to: whether Defendant warranted the Products as "GMO Free"; whether the Products contain genetically modified organisms; whether Defendant breached these warranties; and whether Defendant committed the statutory and common law violations alleged against them herein by doing so.

60. ***Typicality.*** The claims of the named Plaintiff are typical of the claims of the Class and Subclass in that Plaintiff, like all proposed members of the Class and Subclass, had her PII compromised in the Data Breach. Plaintiff and Class and Subclass members were injured in the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arose from the same practices or course of conduct that give rise to the claims of all Class and Subclass members.

61. ***Adequacy.*** Plaintiff is an adequate representative of the Class and Subclass because her interests do not conflict with the interests of the Class and Subclass members she seeks to

represent, she has retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of the Class and Subclass members will be fairly and adequately protected by Plaintiff and her counsel.

62. ***Superiority.*** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class and Subclass members. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of liability issues.

63. Defendant has acted or failed to act on grounds generally applicable to the Class and Subclass, thereby making appropriate final injunctive relief with respect to the Class and Subclass as a whole.

64. Without a class action, Defendant will continue a course of action that will result in further damages to Plaintiff and members of the Class and Subclasses and will likely retain the benefits of its wrongdoing.

65. Based on the foregoing allegations, Plaintiff's claims for relief include those set forth below.

CLAIMS FOR RELIEF

COUNT I
Violations of the Fair Credit Reporting Act ("FCRA"),
15 U.S.C. §§ 1681, *et seq*.
(On Behalf Of The Nationwide Class)

66. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

67. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class against Defendant.

68. Defendant is subject to the FCRA because it is a CRA—a "consumer reporting agency" and a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" as defined in 15 U.S.C. §§ 1681a(f) and (p), respectively.

69. As individuals, Plaintiff and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

70. TransUnion compiled and maintained a "consumer report" on Plaintiff and Class members, as defined in 15 U.S.C. § 1681a(d): any "written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title."

71. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or

expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing Class members' eligibility for credit.

72. As a CRA, TransUnion may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under section 1681b permit CRAs to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Class members' Personal Information.

73. TransUnion furnished Class members' consumer reports, in violation of section 1681b, by disclosing those consumer reports to unauthorized entities and computer hackers, and by allowing unauthorized entities and computer hackers to access their consumer reports.

74. The FCRA requires TransUnion, as a CRA, to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

75. The Federal Trade Commission has pursued enforcement actions against CRAs under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

76. TransUnion failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers.

77. As alleged in detail herein, TransUnion's security practices and procedures were so severely deficient or nonexistent, despite its knowledge that this Personal Information was coveted

by attackers and certain to be subject to attempted hacks and exfiltration, that TransUnion in fact voluntarily and for all practical purposes knowingly offered, provided, and furnished this information to unauthorized third parties.

78. As a direct and proximate result of TransUnion's actions and failures to act described herein, and utter failure to take adequate and reasonable measures to ensure its data systems were protected, TransUnion offered, provided, and furnished Plaintiff's and Class members' consumer reports to unauthorized third parties.

79. TransUnion's disclosure of consumer reports under these circumstances was not permitted by, and thus was in violation of, Sections 1681b and 1681e of the FCRA.

80. As a direct and proximate result of TransUnion's actions and failures to act described herein, and its violation of the FCRA, Plaintiff and Class members have suffered harm and/or face the significant risk of harm suffering such harm in the future, all as described above.

81. Under Section 1681o of the FCRA, TransUnion is liable to Plaintiff and Class members for negligently failing to comply with the requirements that a CRA not disclose consumer reports and take measures designed to avoid the unauthorized disclosure of consumer reports. TransUnion therefore is liable to Plaintiff and Class members for their actual damages as a result of TransUnion's failure to comply with the FCRA, as well as costs and reasonable attorneys' fees, in amounts to be proven at trial.

82. In addition, TransUnion's failure to comply with the foregoing requirements was willful because Equifax knew or should have known, but recklessly disregarded, that its cybersecurity measures were inadequate and unreasonable and additional steps were necessary to protect consumers' Personal Information from security breaches. The willful and reckless nature of TransUnion's violations is supported by, among other things, former employees' admissions

that TransUnion's data security practices have deteriorated in recent years, TransUnion's other data breaches in the past, TransUnion's knowledge of other previous high-profile data breaches, and warnings from cybersecurity experts. Further, TransUnion touts itself as an industry leader in breach prevention; thus, TransUnion was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

83. TransUnion also acted willfully and recklessly because, as a CRA, it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. TransUnion obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Nonetheless, by its utter failure to meet its acknowledged responsibilities and known duties regarding the need to adopt adequate data security measures, TransUnion acted consciously in depriving Plaintiff and Class members of their rights under the FCRA.

84. Therefore, TransUnion is liable to Plaintiff and Class members in an amount equal to actual damages, or damages of not less than $100 and not more than $1,000 for each Plaintiff and Class member, as well as punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a).

COUNT II
Negligence
(On Behalf Of The Nationwide Class And Subclass)

85. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this Complaint.

86. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class and California Subclass against Defendant.

87. TransUnion owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing TransUnion's security systems to ensure that Plaintiff's and Class members' Personal Information in TransUnion's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

88. TransUnion's duty to use reasonable care arose from several sources, including but not limited to those described below.

89. TransUnion had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, TransUnion knew that it was more likely than not Plaintiff and other Class members would be harmed.

90. TransUnion's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable

measures to protect Personal Information by companies such as TransUnion. Various FTC publications and data security breach orders further form the basis of TransUnion's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

91. TransUnion's duty also arose from TransUnion's unique position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. TransUnion undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of TransUnion's data collection activities. TransUnion holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. The consumer public and, indeed, all those who participate in modern American economic life collectively repose a trust and confidence in TransUnion to perform that stewardship carefully. Otherwise consumers would be powerless to fully protect their interests with regard to their Personal Information, which is controlled by TransUnion. Because of its crucial role within the credit system, TransUnion was in a unique and superior position to protect against the harm suffered by Plaintiff and Class members as a result of the TransUnion data breach.

92. TransUnion admits that it has an enormous responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Personal Information at issue here.

93. TransUnion's duty also is based on the FCRA, which reflects Congress's considered judgment that CRAs such as TransUnion hold a unique and superior position in our credit economy, a position that if abused would foreseeably and probably injure consumers like Plaintiff and Class members. The FCRA thus requires that TransUnion maintain reasonable

procedures designed to avoid unauthorized release of information contained in consumer reports, and requires that when issued, consumer reports are complete and accurate.

94. TransUnion also acknowledges and recognizes a pre-existing duty to exercise reasonable care to safeguard Plaintiff's and Class members' Personal Information that extends to those who are entrusted with such information. TransUnion may now deny that it has any legal duty to protect information relating to the data TransUnion maintains relating to Plaintiff and Class Members. But when dealing with businesses that purchase consumer information from TransUnion, TransUnion explicitly recognizes and contractually insists that those businesses have a duty to protect this information.

95. With regard to network security, TransUnion further acknowledges and requires that its business partners must use commercially reasonable efforts to protect TransUnion information when stored on servers.

96. TransUnion also had a duty to safeguard the Personal Information of Plaintiff and Class members and to promptly notify them of a breach because of state laws and statutes that require TransUnion to reasonably safeguard sensitive Personal Information, as detailed herein.

97. Timely notification was required, appropriate and necessary so that, among other things, Plaintiff and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by TransUnion's misconduct.

98. TransUnion breached the duties it owed to Plaintiff and Class members described above and thus was negligent. TransUnion breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and the Class members' Personal Information in TransUnion's possession had been or was reasonably believed to have been, stolen or compromised.

99. But for TransUnion's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Personal Information would not have been compromised.

100. As a direct and proximate result of TransUnion's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiff's and Class members' injuries include:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the TransUnion Data Breach—including finding fraudulent

charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

i. damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to TransUnion with the mutual understanding that TransUnion would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their Personal Information, which remains in TransUnion's possession and is subject to further breaches so long as TransUnion fails to undertake appropriate and adequate measures to protect Plaintiff and Class members; and

k. for purchasers' of TransUnion's own credit monitoring and identity theft protection products, diminution of the value and/or loss of the benefits of those products.

COUNT III
Negligence *Per Se*
(On Behalf Of The Nationwide Class And Subclass)

101. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this Complaint.

102. Plaintiff brings this claim individually and on behalf of the members of the proposed Nationwide Class and California Subclass against Defendant.

103. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as TransUnion of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Equifax's duty.

104. TransUnion violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry

standards. TransUnion's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach at one of the three major credit bureaus.

105. TransUnion's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

106. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

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

108. As a direct and proximate result of TransUnion's negligence, Plaintiff and Class members have been injured as described herein and in Paragraph above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT IV
Violations of California's Unfair Competition Law ("UCL"), California Business & Professions Code §§ 17200, et seq. (On Behalf Of The California Subclass)

109. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this Complaint.

110. Plaintiff brings this claim individually and on behalf of the members of the proposed California Subclass against Defendant.

111. TransUnion is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

112. TransUnion violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

113. TransUnion's "unfair" acts and practices include:

a. TransUnion failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the TransUnion Data Breach. TransUnion failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. TransUnion's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), the Gramm-Leach Bliley Act (15 U.S.C. § 6801(a)), California's Consumer Records Act (Cal. Civ. Code §§ 1798.81.5, *et seq*.), and California's Consumer Credit Reporting Agencies Act (Cal. Civ. Code §§ 1785.1, *et seq*.).

c. TransUnion's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of TransUnion's inadequate security, consumers could not have reasonably avoided the harms that TransUnion caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code §§ 1798.82 *et seq*., and Cal. Civ. Code §§ 1785.1, *et seq*.

114. TransUnion has engaged in "unlawful" business practices by violating multiple laws, including: California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); California's Consumer Credit Reporting Agencies Act ("CCRAA"), Cal. Civ. Code §§ 1785.1, *et seq*.; California's Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1780, *et seq*. (alleged

below); the FCRA, 15 U.S.C. §§ 1681e (alleged above); the FTC Act, 15 U.S.C. § 45; and California common law.

115. TransUnion's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California Subclass members' Personal Information, which was a direct and proximate cause of the TransUnion Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the TransUnion Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; the FCRA, 15 U.S.C. § 1681e; the CCRAA, Cal. Civ. Code §§ 1785.1, *et seq*.; and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., which was a direct and proximate cause of the TransUnion Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; the FCRA, 15 U.S.C. § 1681e; the CCRAA, Cal. Civ. Code §§ 1785.1, *et seq*.; and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; the FCRA, 15 U.S.C. § 1681e; the CCRAA, Cal. Civ. Code §§ 1785.1, *et seq*.; and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.

116. TransUnion's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of TransUnion's data security and ability to protect the confidentiality of consumers' Personal Information.

117. As a direct and proximate result of TransUnion's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including the costs passed through to TransUnion from their consumer credit transactions, the premiums and/or price received by TransUnion for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

118. TransUnion acted intentionally, knowingly, and maliciously to violate California's UCL, and it recklessly disregarded Plaintiff's and California Subclass members' rights. TransUnion's past data breaches put it on notice that its security and privacy protections were inadequate.

119. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from TransUnion's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT V
Violation Of California's Consumers Legal Remedies Act ("CLRA"), California Civil Code §§ 1750, *et seq*. (On Behalf Of The California Subclass)

120. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this Complaint.

121. Plaintiff brings this claim individually and on behalf of the members of the proposed California Subclass against Defendant.

122. The Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, *et seq*., is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

123. TransUnion s a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

124. Plaintiff and members of the California Subclass are "consumers" within the meaning of Cal. Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

125. TransUnion's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

126. The acts and practices of Defendant as described above were intended to deceive Plaintiff and the California Subclass as described herein, and have resulted, and will continue to result, in damages to Plaintiff and members of the California Subclass. These actions violated, and continue to violate, the CLRA in at least the following respects: (a) Defendant's acts and practices constitute representations deceiving that the Products have characteristics, uses, and/or benefits, which they do not have, in violation of Cal. Civil Code § 1770(a)(5); (b) Defendant's acts and practices constitute representations that the Products are of a particular standard, quality, or grade, when in fact they are of another, in violation of Cal. Civil Code § 1770(a)(7); (c) Defendant's acts and practices constitute the advertisement of the Products in question with the

intent not to sell them as advertised, in violation of Cal. Civil Code § 1770(a)(9); and (d) Defendant's acts and practices constitute representations that the subject of a transaction has been supplied in accordance with a previous representation when it has not in violation of Cal. Civil Code § 1770(a)(16).

127. TransUnion's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of TransUnion's data security and ability to protect the confidentiality of consumers' Personal Information.

128. Has TransUnion disclosed to Plaintiff and California Subclass members that its data systems were not secure and, thus, vulnerable to attack, TransUnion would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, TransUnion held itself out as one of the three nationwide credit-reporting companies that serve as trusted linchpins of the financial system, and TransUnion was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the California Subclass. TransUnion accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public. Accordingly, because TransUnion held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Plaintiff and the California Subclass members acted reasonably in relying on TransUnion's misrepresentations and omissions, the truth of which they could not have discovered.

129. As a direct and proximate result of Equifax's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

130. Plaintiff, on behalf of herself and all other members the California Subclass, seeks an injunction prohibiting Defendant from continuing its unlawful practices in violation of the CLRA.

COUNT VI
Unjust Enrichment / Restitution
(On Behalf Of The Nationwide Class And Subclass)

131. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

132. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class and Subclass against Defendant.

133. To the extent the Court determines it is necessary to do so, this claim is pled in the alternative to the other legal claims alleged in the complaint.

134. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by TransUnion and that was ultimately stolen in the TransUnion Data Breach. This Personal Information was conferred on TransUnion in most cases by third-parties but in some instances directly by Plaintiff and/or Class members themselves.

135. TransUnion was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiff and Class members and by its ability to retain and use that information. TransUnion understood that it was in fact so benefitted.

136. TransUnion also understood and appreciated that the Personal Information pertaining to Plaintiff and Class members was private and confidential and its value depended upon TransUnion maintaining the privacy and confidentiality of that Personal Information.

137. But for TransUnion's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with TransUnion. Further, if TransUnion had disclosed that its data security measures were inadequate, Equifax would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

138. As a result of TransUnion's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), TransUnion has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members. Among other things, TransUnion continues to and profit from the sale of the Personal Information while its value to Plaintiff and Class members has been diminished.

139. TransUnion's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

140. Under the common law doctrine of unjust enrichment, it is inequitable for TransUnion to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner.

TransUnion's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

141. The benefit conferred upon, received, and enjoyed by TransUnion was not conferred officiously or gratuitously, and it would be inequitable and unjust for TransUnion to retain the benefit.

142. TransUnion is therefore liable to Plaintiff and Class members for restitution in the amount of the benefit conferred on TransUnion as a result of its wrongful conduct, including specifically the value to TransUnion of the Personal Information that was stolen in the TransUnion Data Breach and the profits TransUnion is receiving from the use and sale of that information.

COUNT VII
Declaratory Judgment
(On Behalf Of The Nationwide Class And Subclass)

143. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

144. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class and Subclass against Defendant.

145. 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 grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

146. An actual controversy has arisen in the wake of the TransUnion Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether TransUnion is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that

compromise their Personal Information. Plaintiff alleges that TransUnion's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of their Personal Information and remains at imminent risk that further compromises of her Personal Information will occur in the future.

147. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. TransUnion continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b. TransUnion continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

148. The Court also should issue corresponding prospective injunctive relief requiring TransUnion to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

149. If an injunction is not issued, Plaintiff will suffer irreparable injury, and she lacks an adequate legal remedy in the event of another data breach at TransUnion. The risk of another such breach is real, immediate, and substantial. If another breach at TransUnion occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

150. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to TransUnion if an injunction is issued. Among other things, if another massive data breach occurs at TransUnion, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to TransUnion of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and TransUnion has a pre-existing legal obligation to employ such measures.

151. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at TransUnion, thus eliminating the additional injuries that would result to Plaintiff and the millions of consumers whose confidential information would be further compromised.

REQUEST FOR RELIEF

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

(a) For an order certifying the Nationwide Class and the California Subclass under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representatives of the Class and Subclass, and naming Plaintiff's attorneys as Class Counsel to represent the proposed Class and Subclass;

(b) For an order declaring that Defendant's conduct violates the statutes and laws referenced herein;

(c) For an order finding in favor of Plaintiff, the Class, and the Subclass on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For injunctive relief as pleaded or as the Court may deem proper;

(h) For an order awarding Plaintiff and members of the Class and Subclass their reasonable attorneys' fees and reimbursement of litigation expenses and costs of suit; and

(i) For such other and further relief as the Court may deem proper.

Dated: November 28, 2022

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Email: gklinger@milberg.com

Nick Suciu III
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
6905 Telegraph Road, Suite 115
Bloomfield Hills, MI 48301
Tel: (313) 303-3472
Email: nsuciu@milberg.com

BURSOR & FISHER, P.A.
Philip L. Fraietta
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: pfraietta@bursor.com

BURSOR & FISHER, P.A.
Julia K. Venditti (*Pro Hac Vice Forthcoming*)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: jvenditti@bursor.com

Attorneys for Plaintiff and the Putative Class

CLRA Venue Declaration Pursuant to California Civil Code Section 1780(d)

I, Gary M. Klinger, declare as follows:

1. I am an attorney at law licensed to practice in the State of Illinois and a member of the bar of this Court. I am a Partner at Milberg Coleman Bryson Phillips Grossman PLLC, counsel of record for Plaintiff Theresa Bryant. Plaintiff Bryant resides in Los Angeles, California. I have personal knowledge of the facts set forth in this declaration and, if called as a witness, I could and would competently testify thereto under oath.

2. The Complaint filed in this action is filed in the proper place for trial under Civil Code Section 1780(d) in that a substantial portion of the events alleged in the Complaint occurred in the Northern District of Illinois. Additionally, Defendant maintains its principal place of business in this District, and Defendant's unlawful conduct and a substantial portion of the acts, practices, and events that gave rise to Plaintiff's claims occurred in this District.

I declare under the penalty of perjury under the laws of the State of Illinois and the United States that the foregoing is true and correct and that this declaration was executed at Chicago, Illinois, this 28th day of November, 2022.

/s/ Gary M. Klinger
Gary M. Klinger