WARREN TERZIAN LLP
Thomas D. Warren (0077541)
30799 Pinetree Rd., Suite 345
Pepper Pike, OH 44124
Tel: (216) 304-4970
tom.warren@warrenterzian.com

Thomas E. Loeser (*pro hac vice to be filed*)
Ellen J Wen (*pro hac vice to be filed*)
COTCHETT, PITRE & McCARTHY, LLP
1809 7th Ave., Ste. 1610
Seattle, WA 98101
Tel.: (206) 802-1272
tloeser@cpmlegal.com
ewen@cpmlegal.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF OHIO

CHARLES BUCKLES, individually and on behalf of all others similarly situated, Plaintiff, v. NAVIGATE360, LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Plaintiff Charles Buckles, individually and on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendant Navigate360, LLC ("Navigate360" or "Defendant"), seeking monetary damages, restitution, and/or injunctive relief for the proposed Class and Subclasses, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of counsel, and personal knowledge or facts that are a matter of public record.

I. INTRODUCTION

1. The release, disclosure, and publication of sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach—with the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain government benefits, and/or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

2. Plaintiff and Class Members are crime reporters, confidential informants and tipsters who report crime and bring about justice – potentially risking their lives. Defendant's failure to implement even basic cybersecurity safeguards has led to the disclosure of the identities and Personally Identifiable Information ("PII") of purportedly anonymous informants and reporters, with potentially devastating consequences. Beyond the already devastating impacts of a conventional data breach, Plaintiff and Class Members now face the immediate threat of retaliation and potentially physical violence.

3. Crime Stoppers and P3 Global Intel, which provides the infrastructure for the decentralized network of Crime Stoppers, have long been synonymous with the supposedly ironclad promise of anonymity. This promise was a cornerstone of their operations. Defendant and Crime Stoppers promised Plaintiff and the Class that "the community provides anonymous tips by using the P3Tips mobile phone app."[2] Defendant Navigate360 is the owner of P3 Global Intel. Defendant hosted and facilitated Crime Stoppers branches across the country and internationally and promised anonymity.

4. Plaintiff and Class Members were ensured that they "never ask for the tipster's

---

[1] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, 25 S.C. LAWYER 28-35 (May 2014), https://law-journals-books.vlex.com/vid/data-breaches-0514-scbj-625743678 (behind paywall) (last visited Nov. 12, 2025).

[2] https://crimestoppers.com/ (last visited Mar. 20, 2026).

name, and it's this anonymity that enables people to offer a tip without the fear of retaliation."[3] Defendant is acutely aware of the extreme sensitivity of Plaintiff and Class Members' PII and that this anonymity protected tipsters against the threat of physical retaliation. Defendant's own sales material restated that "each tipster's identity will remain anonymous at all times."[4]

5. This promise was a lie. Plaintiff and Class Members did not remain anonymous, Defendant did in fact gather PII about Plaintiff and the Class, and this extremely sensitive information was exfiltrated from Defendant's servers (the "Data Breach").[5]

6. Even though Defendant promised anonymity, Defendant gathered and failed to adequately protect Plaintiff's highly sensitive PII. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing potentially life-threatening risk to victims of the Data Breach will remain for their respective lifetimes.

7. The data exposed in the Data Breach includes at least "names, email addresses, dates of birth, phone numbers, home addresses, license plate numbers, Social Security numbers and criminal histories."[6]

8. As a result of the Data Breach, through which their Personally Identifiable Information ("PII") was compromised, disclosed, and obtained by unauthorized third parties, Plaintiff and Class Members have suffered concrete damages and are now exposed to heightened and imminent risk of fraud, identity theft, and violence for a period of years, if not decades. Furthermore, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiff and

---

[3] *Id.*
[4] P3 Global Intel, Pre-Sales / Frequently Asked Questions, P3 GLOBAL INTEL https://p3intel.com/index_htm_files/P3%20PreSales%20FAQ%202016.pdf (last visited Mar. 20, 2026).
[5] Mikael Thalen, *Millions of 'anonymous' crime tips exposed in massive Crime Stoppers hack: Exclusive*, STRAIGHT ARROW NEWS (Mar. 18, 2026), https://san.com/cc/millions-of-anonymous-crime-tips-exposed-in-massive-crime-stoppers-hack-exclusive/ (last visited Mar. 20, 2026).
[6] *Id.*

the other victims will incur ongoing out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft and ensure their ongoing physical safety.

9. The sensitivity of Plaintiff and victims' exfiltrated information cannot be overstated. In one instance, a Class Member was aware of the Sinaloa Drug Cartel trafficking hundreds of pounds of drugs, and wrote "Please, this must remain anonymous… so if captured, do not say it was from a tip cause they would know where it came from."[7] It is clear that the unique risk associated with Defendant's Data Breach "include[s] severe harm and even death to police informants."[8]

10. By this Complaint, Plaintiff seeks to remedy these harms on behalf of himself, and all similarly situated individuals whose PII was accessed during the Data Breach.

II. PARTIES

A. Plaintiff Charles Buckles

11. Plaintiff Charles Buckles is a citizen of and is domiciled in the state of Louisiana.

12. Plaintiff submitted information to Crime Stoppers Tangipahoa, which uses Navigate360 to manage submission of purportedly secured information.

13. Plaintiff provided confidential and sensitive PII to Defendant when submitting information about a crime, as requested and required by Defendant. Defendant obtained and continues to maintain Plaintiff's PII and has a legal duty and obligation to protect that PII from unauthorized access and disclosure.

14. Plaintiff would not have entrusted his PII to Defendant had he known that Defendant failed to maintain adequate data security.

15. Plaintiff subsequently spent time taking action to mitigate the impact of the Data Breach, including researching the Data Breach, researching ways to protect himself from the Data Breach. Now he plans to spend time checking account statements for irregularities on an ongoing

---

[7] *Id.*
[8] *Id.*

basis.

16. As a result of the Data Breach, Plaintiff has suffered emotional distress from the release of his PII, which he expected Defendant to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing and potentially using his PII. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money to contain the impact of the Data Breach.

B. Defendant

17. Defendant Navigate360, LLC is organized in Nevada with its principal place of business at 3900 Kinross Lakes Parkway, Suite 200, Richfield, Ohio. Navigate360 purchased P3 Global Intel in 2020, which provides tip acquisition and management software to Crime Stoppers Programs, law enforcement, school safety programs, and US federal agencies.[9] P3 Global Intel is now a division of Navigate360.

18. P3 Global Intel joined Navigate360 in 2020.[10] As a division of Navigate360, P3 Global Intel is described as "an arm of safety company Navigate360" and Navigate360's "tip line."[11] On information and belief P3 Global Intel has no functions independent of Navigate360 and is entirely run from the Navigate360 headquarters in Richfield, Ohio.

III. JURISDICTION AND VENUE

19. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below,

---

[9] Navigate360, *Navigate360 Adds P3 Global Intel to Further Expand its Portfolio of World Class Safety Solutions*, PR NEWSWIRE (Sep. 23, 2020), https://www.prnewswire.com/news-releases/navigate360-adds-p3-global-intel-to-further-expand-its-portfolio-of-world-class-safety-solutions-301136545.html (last visited Mar. 20, 2026).

[10] https://www.prnewswire.com/news-releases/navigate360-adds-p3-global-intel-to-further-expand-its-portfolio-of-world-class-safety-solutions-301136545.html (last visited Mar. 30, 2026).

[11] https://www.reuters.com/legal/government/hacker-says-they-compromised-millions-confidential-police-tips-held-by-us-2026-03-18/ (last visited Mar. 30, 2026); https://www.edweek.org/technology/a-potential-breach-of-an-anonymous-tip-app-could-have-exposed-sensitive-student-data/2026/03 (last visited Mar. 30, 2026).

and minimal diversity exists because at least one Plaintiff is a citizen of a state different from the citizenship of Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1367.

20. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District, has sufficient minimum contacts with this District, and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

21. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events or omissions giving rise to the claims occurred in this district—this is where Defendant's principal place of business is located and conducts substantial business, including its actions and inactions leading to the data breach at issue. Defendant also gains revenue and profits from doing business in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant Falsely Promised Anonymity And Security

22. Crime Stoppers and Navigate360 promised Plaintiff and Class Members that they can "report tips and engage in fully anonymous dialogue through a mobile app, desktop or mobile browser, or telephone."[12] Navigate360's home page highlights their "anonymous reporting system."[13] The home page of P3 Global Intel Tip Management Software similarly highlights "anonymous two way communication with [] tipsters,"[14] "the P3 platform enables the public to share information anonymously with Crime Stoppers programs,"[15] and the P3 Frequently Asked Questions promises that the "tipster's identity will remain anonymous at all times."[16] Crime Stoppers further highlights that they facilitate "anonymous tips by using the P3Tips mobile phone

[12] *Id.*; https://crimestoppers.com/ (last visited Mar. 20, 2026).
[13] https://navigate360.com/ (last visited Mar. 23, 2026).
[14] https://www.p3intel.com/ (last visited Mar. 23, 2026).
[15] https://www.p3tips.com/community/index.htm (last visited Mar. 23, 2026).
[16] *Frequently Asked Questions,* P3 Global Intel, https://p3intel.com/index_htm_files/P3%20PreSales%20FAQ%202016.pdf (last visited Mar. 23, 2026).

app, by visiting our site, or by calling."[17]

Figure 1 – Home Page of the P3Tips App used to submit purportedly anonymous tips that links back to Crime Stopper's website.

23. Defendant and Crime Stoppers' representations regarding anonymity are inextricably linked. Crime Stoppers has Plaintiff and Class Members submit their tips "online at P3Tips.com… [or] on the P3Tips app."[18] Once on the homepage of the P3Intel App, users are referred back to the Crime Stoppers web page wherein users are again presented with Crime Stopper's promises about anonymity.

[17] https://crimestoppers.com/ (last visited Mar. 20, 2026).
[18] https://crimestoppers.com/submit-a-tip/ (last visited Mar. 20, 2026).

24. Navigate360 itself also made promises regarding Plaintiff's anonymity, it directly routed Plaintiff and Class Members to Crime Stoppers websites which further promised anonymity, and the links and branding of both Crime Stoppers and Defendant are highly integrated among each party's advertising and platforms. A reasonable consumer would have understood Defendant and Crime Stoppers' representations as a promise of anonymity when submitting a tip, and a reasonable consumer would not have entrusted his PII with Defendant if he knew that it actually collected or retained his PII and did not implement reasonable security measures.

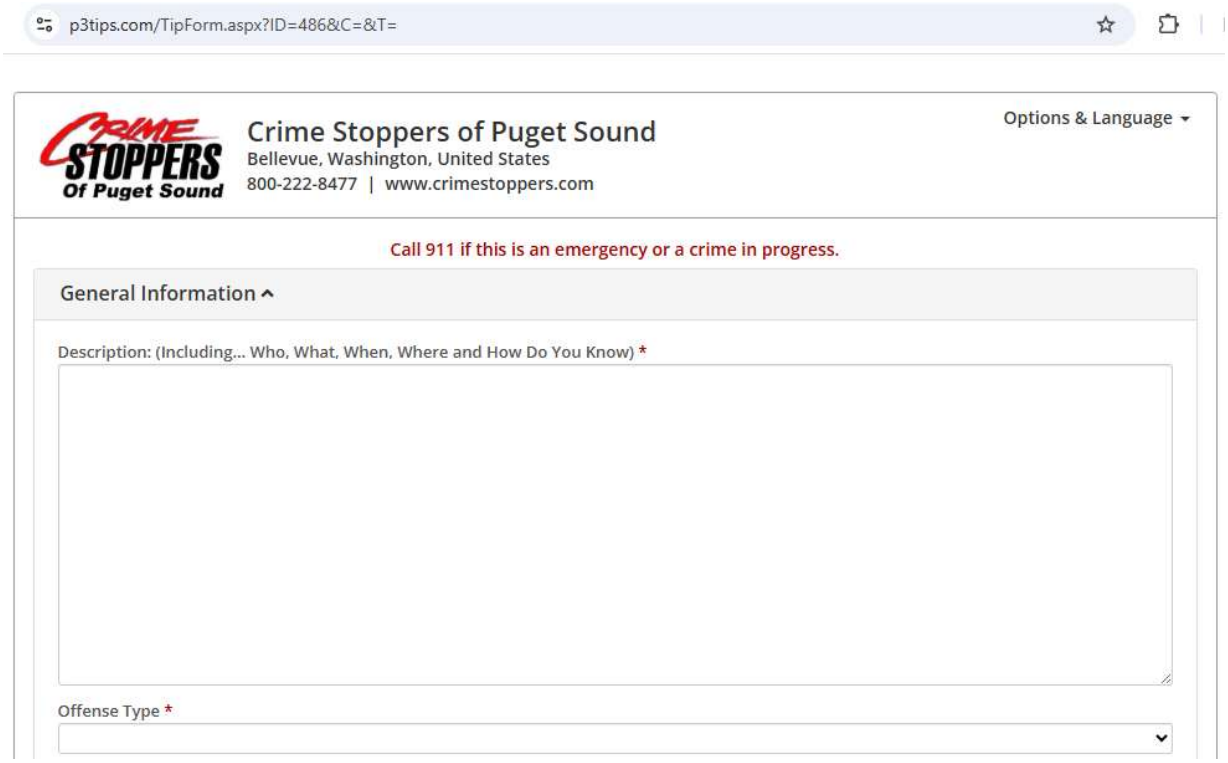

Figure 2 – P3Tips purportedly anonymous online tip platform including Crime Stoppers branding

25. Defendant's promises were false. Defendant, in fact, gathered and insufficiently secured consumers' "names, email addresses, dates of birth, phone numbers, home addresses, license plate numbers, Social Security numbers and criminal histories"[19] as well as substantive

[19] Mikael Thalen, *Millions of 'anonymous' crime tips exposed in massive Crime Stoppers hack: Exclusive*, STRAIGHT ARROW NEWS (Mar. 18, 2026), https://san.com/cc/millions-of-anonymous-crime-tips-exposed-in-massive-crime-stoppers-hack-exclusive/ (last visited Mar. 20, 2026).

communications from investigators.[20]

26. Moreover, Defendant even detailed how its clients, like Crime Stoppers, could "track tipsters without their knowledge."[21] Defendant knew of the vital importance of consumer anonymity, falsely promised this anonymity, and even secretly tracked these consumers under the guise of consumer security.

A. Navigate360 Failed to Adequately Protect Customer Data, Resulting in the Data Breach

27. In the course of its business, Defendant collects PII, directly or indirectly, from consumers like Plaintiff.

28. As a condition of providing services, Defendant receives, creates, and handles the PII of Plaintiff and Class Members.

29. Plaintiff and Class Members must provide Defendant with their sensitive and confidential PII to receive Defendant's services. Plaintiff reasonably expected that Defendant would safeguard his highly sensitive information and keep it confidential.

30. Due to the sensitivity of the PII that Defendant handles, Defendant is aware of its critical responsibility to safeguard this information—and, therefore, how devastating its theft is to individuals whose information has been stolen.

31. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed equitable and legal duties to safeguard and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

32. Despite the existence of these duties, Defendant failed to implement reasonable data security measures to protect the information with which it was entrusted and ultimately

---

[20] Nate Anderson, *Internet Yiff Machine: We hacked 93GB of 'anonymous' crime tips*, ARSTECHNICA (Mar. 26, 2026), https://arstechnica.com/security/2026/03/internet-yiff-machine-we-hacked-93gb-of-anonymous-crime-tips/ (last visited Mar. 27, 2026).

[21] Mikael Thalen, *Millions of 'anonymous' crime tips exposed in massive Crime Stoppers hack: Exclusive*, STRAIGHT ARROW NEWS (Mar. 18, 2026), https://san.com/cc/millions-of-anonymous-crime-tips-exposed-in-massive-crime-stoppers-hack-exclusive/ (last visited Mar. 20, 2026).

allowed nefarious third-party hackers to compromise Plaintiff's and Class Members' PII.

33. There are likely tens if not hundreds of thousands of users who do not yet know that their information was impacted by this data breach.

B. Defendant Failed To Secure Customer PII.

34. On the Privacy Policy of its website, Defendant states "Navigate360 takes your right to privacy seriously and wants you to feel comfortable using this website and any Navigate 360 products or services."[22]

35. Defendant made these representations because it knows and understands the severe consequences of losing sensitive PII.

36. Notwithstanding these promises, on March 18, 2026, a hacker group leaked over 8.3 million highly sensitive records of tipsters ranging approximately 38 years.[23] These records included the substance of tips themselves, user account details,[24] names, social security numbers, license plate numbers, home addresses, and criminal histories.[25]

37. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[26] And this particular data, the identity of persons who reported crimes, could be highly valuable to criminal organizations in discovering or rooting out informants, with potentially devastating results to the lives and well-being of those affected.

---

[22] https://navigate360.com/policies/privacy/ (last visited March 23, 2026).
[23] Mikael Thalen, *Millions of 'anonymous' crime tips exposed in massive Crime Stoppers hack: Exclusive*, Straight Arrow News (Mar. 18, 2026), https://san.com/cc/millions-of-anonymous-crime-tips-exposed-in-massive-crime-stoppers-hack-exclusive/ (last visited Mar. 20, 2026).
[24] Dominykas Zukas, Millions Trusted Crime Stoppers With Their Safety, and the Platform Was Quietly Logging Them, MYSTERIUM VPN (Mar. 19, 2026), https://www.mysteriumvpn.com/blog/news/crime-stoppers-hack-exposes-millions-anonymous-tips (last visited Mar. 27, 2026).
[25] Mikael Thalen, *Millions of 'anonymous' crime tips exposed in massive Crime Stoppers hack: Exclusive*, Straight Arrow News (Mar. 18, 2026), https://san.com/cc/millions-of-anonymous-crime-tips-exposed-in-massive-crime-stoppers-hack-exclusive/ (last visited Mar. 20, 2026).
[26] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited Mar. 30, 2026).

38. Navigate360 was familiar with its obligations—created by contract, industry standards, common law, and representations to its customers—to protect customer and employee information. Plaintiff and Class Members provided their PII to Navigate360 with the reasonable expectation that Navigate360 would comply with its obligations to keep such information confidential and secure.

39. Navigate360 failed to comply with these obligations, resulting in the Data Breach. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records and the ongoing fear that persons investigated, prosecuted or potentially jailed as a result of their tips to law enforcement, might learn their identity and seek retribution.

C. Defendant Failed to Comply with Regulatory Guidance and Industry-Standard Cybersecurity Practices

40. Defendant's data security failure stems from its failure to comply with state law and federal laws and requirements as well as industry standards governing the protection of PII.

41. At least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain PII to implement and maintain reasonable security procedures and practices and to protect PII from unauthorized access.

42. Defendant also failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

43. The FTC recommends:

- Limiting access to customer information to employees who have a business reason to see it;
- keeping customer information in encrypted files provides better protection in case of theft;
- maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;

- using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;
- monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and
- monitoring activity logs for signs of unauthorized access to customer information.[27]

44. The FTC has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

45. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[29] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

---

[27] Federal Trade Commission, *FTC Safeguards Rule: What Your Business Needs to Know*, available at https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know (last visited Mar. 30, 2026).

[28] Federal Trade Commission, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Mar. 30, 2026).

[29] Federal Trade Commission, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 30, 2026).

47. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

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

49. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

50. According to the Federal Bureau of Investigation (FBI), phishing schemes designed to induce individuals to reveal personal information, such as network passwords, were the most common type of cybercrime in 2020, with such incidents nearly doubling in frequency between 2019 and 2020.[30] According to Verizon's 2021 Data Breach Investigations Report, 43% of breaches stemmed from phishing and/or pretexting schemes.[31]

51. Defendant was aware of its obligations to protect customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect its customers and employees from unauthorized access. In this case, Defendant was at all times fully aware of its obligation to protect the PII of its customers because it marketed P3 Global Intel as "THE PIONEER OF TIP MANAGEMENT SOFTWARE" and provides "[a] fully integrated and state-of-the-art tip acquisition and tip management solution that has quickly become the leading choice

---

[30] *2020 Internet Crime Report*, FBI, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (last visited Nov. 6, 2025).
[31] *2021 DBIR Master's Guide*, VERIZON, https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (subscription required) (last visited June 28, 2024).

of Crime Stoppers Programs, Law Enforcement Agencies, Campus Safety Programs, and Federal Agency Initiatives."[32] Defendant was also aware of the significant repercussions if it failed to do so because Defendant collected PII from millions of tipsters and crime reporters and knew that this PII, if hacked, would result in financial and potential physical injury to consumers, including Plaintiff and Class Members.

52. Based upon the known details of the Data Breach and how it occurred, Defendant also failed to comply with industry-standard cybersecurity practices, including, but not limited to, proper firewall configuration, network segmentation, secure credential storage, rate limiting, user-activity monitoring, data-loss prevention, and intrusion detection and protection.

D. The Breach Increases The Risk of Fraud, Identity Theft, and Physical Harm

53. Defendant's failure to keep Plaintiff's and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach— names, email addresses, dates of birth, phone numbers, home addresses, license plate numbers, Social security numbers, and criminal histories—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. Moreover, tipsters may themselves be vulnerable members of the community who may not be comfortable reporting crimes against them personally, if they are targeted. As a result, Plaintiff has suffered injury and faces an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

54. There is little doubt that victims' PII from the Data Breach will be circulating on the dark web, as it is highly valuable. Malicious actors use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[33]

---

[32] https://www.p3intel.com/ (last visited March 23, 2026).

[33] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

55. Further, identity thieves often wait months or years to use PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some Class Members' data may have been compromised in other data breaches, the fact that the Breach centralizes the PII and identifies the victims as tipsters or crime reporters materially increases the risk to Plaintiff and the Class.

56. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[34] Moreover, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. Plaintiff will therefore need to spend time and money to continuously monitor his accounts for years to ensure the PII obtained in the Data Breach is not used to harm him. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach. In other words, Plaintiff and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

57. Plaintiff and Class Members have also realized harm in the lost or reduced value of their PII. Defendant admits the PII compromised in the Breach is valuable. Defendant collects, retains, and uses Plaintiff's and Class Members' PII to earn revenue. Plaintiff's and Class Members' PII is not only valuable to Defendant, but Plaintiff and Class Members also place value on their PII based on the understanding that their PII is a financial asset to companies who collect

[34] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (2007), https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited Mar. 30, 2026).

it.[35]

58. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's unauthorized access to Plaintiff's PII that was permitted without authorization by Defendant. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

59. Moreover, Plaintiff and Class Members value the privacy of this information and expect Defendant to allocate enough resources to ensure it is adequately protected. Plaintiff and other crime reporters and tipsters would not have provided Defendant their PII had they known Defendant did not implement reasonable security measures to protect their PII.[36]

60. Given Defendant's failure to protect consumers' PII, Plaintiff and the Class Members have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII remains in Defendant's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

61. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) loss of value of their PII; (iv) the lost value of unauthorized access to Plaintiff's and Class Members' PII permitted by Defendant; (v) the amount of the actuarial present value of ongoing

---

[35] *See, e.g.*, Ponemon Institute, LLC, *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, its Social Security number at $55.70), available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html.

[36] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://storage.ghost.io/c/74/27/74275281-39ba-4091-be76-0573d609c246/content/files/2024/03/rpt-beyond-bottomline.pdf (last visited March 30, 2026) (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (vi) Defendant's retention of profits attributable to Plaintiff's and Class Members' PII that Defendant failed to adequately protect; (vii) the certain, imminent, and ongoing threat of fraud, identity theft, and physical harm, including the economic and non-economic impacts that flow therefrom; (viii) ascertainable out-of-pocket expenses and the value of its time allocated to fixing or mitigating the effects of the Data Breach; and (ix) nominal damages.

V. CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action as a class under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed nationwide class (the "Class"), defined as:

Nationwide Class:

> All natural persons in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

State Subclass:

> All natural persons in the State of Louisiana whose Personally Identifiable Information was compromised as a result of the Data Breach.

63. Plaintiff reserves the right to amend the class definition.

64. **Numerosity and Ascertainability:** Plaintiff does not know the exact size of the Class or identity of the Class Members, since such information is in the exclusive control of Defendant. Nevertheless, the Class encompasses millions of individuals dispersed throughout the United States. The number of Class Members is so numerous that joinder of all Class Members is impracticable. The names, addresses, and phone numbers of Class Members are identifiable through documents maintained by Defendant.

65. **Commonality and Predominance:** This action involves common questions of law and fact which predominate over any question solely affecting individual Class Members.

66. These common questions include:

a) whether Defendant engaged in the conduct alleged herein;

b) whether Defendant had a legal duty to use reasonable security measures to protect Plaintiff's and Class Members' PII;

c) whether Defendant timely, accurately, and adequately informed Plaintiff and Class Members that their PII had been compromised;

d) whether Defendant breached their legal duty by failing to protect the PII of Plaintiff and Class Members;

e) whether Defendant acted reasonably in securing the PII of Plaintiff and Class Members;

f) whether Plaintiff and Class Members are entitled to injunctive relief; and

g) whether Plaintiff and Class Members are entitled to damages and equitable relief.

67. **Typicality:** Plaintiff's claims are typical of the other Class Members' claims because all Class Members were comparably injured through Defendant's substantially uniform misconduct, as described above. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other members of the Class that he represents, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and Class Members arise from the same operative facts and are based on the same legal theories.

68. **Adequacy:** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other members of the Class he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action vigorously. The Class's interest will be fairly and adequately protected by Plaintiff and his counsel.

69. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other detriment suffered by Plaintiff and other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be virtually impossible for the Class Members to individually seek redress for Defendant's wrongful conduct. Even if

Class Members could afford individual litigation, the court system could not: individualized litigation creates a potential for inconsistent or contradictory judgments, increases the delay and expense to the parties, and increases the expense and burden to the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by this Court.

VI. CAUSES OF ACTION

A. Claims Brought on Behalf of the Nationwide Class, or in the alternative, the Louisiana State Subclass.

FIRST CAUSE OF ACTION
NEGLIGENCE

70. Plaintiff incorporates the foregoing allegations 1 to 69 as if fully set herein.

71. Navigate360 requires users to submit non-public PII as a condition of its services. Navigate360 gathered and stored the PII of Plaintiff and Class Members as part of its business.

72. Navigate360 owed a duty to Plaintiff and Class Members, arising from the sensitivity of the information, the expectation the information was going to be kept private, and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' information was adequately secured from unauthorized access.

73. Navigate360's Privacy Policy acknowledged its duty to adequately protect Plaintiff's and Class Members' PII.

74. Navigate360 owed a duty to Plaintiff and Class Members to implement administrative, physical and technical safeguards, such as intrusion detection processes that detect data breaches in a timely manner, to protect and secure Plaintiff's and Class Members' PII.

75. Navigate360 also had a duty to maintain only necessary PII.

76. Navigate360 owed a duty to disclose the material fact that its data security practices

were inadequate to safeguard Plaintiff's and Class Members' PII.

77. Navigate360 also had independent duties under Plaintiff's and Class Members' state laws that required Navigate360 to reasonably safeguard Plaintiff's and Class Members' PII, and promptly notify them about the Data Breach.

78. Navigate360 had a special relationship with Plaintiff and Class Members as a result of being entrusted with their PII, which provided an independent duty of care. Plaintiff's and Class Members' willingness to entrust Navigate360 with their PII was predicated on the understanding that Navigate360 would take adequate security precautions. Moreover, Navigate360 was capable of protecting its networks and systems, and the PII it stored on them, from unauthorized access.

79. Navigate360 breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Plaintiff's and Class Members' PII, including administrative, physical, and technical safeguards; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that its data security practices were inadequate to safeguard Plaintiff's and Class Members' PII.

80. But for Navigate360's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII would not have been accessed by unauthorized parties.

81. Plaintiff and Class Members were foreseeable victims of Navigate360's inadequate data security practices. Navigate360 knew or should have known that a breach of its data security systems would cause damage to Plaintiff and Class Members.

82. It was reasonably foreseeable that the failure to reasonably protect and secure Plaintiff's and Class Members' PII would result in unauthorized access to Navigate360's networks, databases, and computers that stored or contained Plaintiff's and Class Members' PII.

83. As a result of Navigate360's negligent failure to prevent the Data Breach, Plaintiff and Class Members suffered injury, which includes, but is not limited to, exposure to a heightened and imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against

identity theft. Plaintiff and Class Members have also incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter and detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and Class Members are also at increased risk of physical harm as a result of the Data Breach.

84. The harm to Plaintiff and Class Members was a proximate, reasonably foreseeable result of Navigate360's breaches of its aforementioned duties.

85. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

86. Plaintiff incorporates the foregoing allegations 1 to 69 as if fully set forth herein.

87. Under the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Navigate360 had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

88. In addition, under state data security statutes, Navigate360 had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' PII.

89. Defendant breached its duties to Plaintiff and Class Members, under the Federal Trade Commission Act, 15 U.S.C. § 45, ("FTCA") and the state data security statutes, by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

90. Plaintiff and Class Members were foreseeable victims of Navigate360's violations of the FTCA and state data security statutes. Navigate360 knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' PII would cause damage to Plaintiff and Class Members.

91. Navigate360's failure to comply with the applicable laws and regulations

constitutes negligence per se.

92. But for Navigate360's failure to comply with applicable laws and regulations, Plaintiff and Class Members suffered injury, which includes but is not limited to the exposure to a heightened and imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and Class Members are also at increased risk of physical harm as a result of the Data Breach.

93. The harm to Plaintiff and the Class Members was a proximate, reasonably foreseeable result of Navigate360's breaches of the applicable laws and regulations.

94. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
GROSS NEGLIGENCE

95. Plaintiff incorporates the foregoing allegations 1 to 69 as if fully set forth herein.

96. Plaintiff and Class Members entrusted Navigate360 with highly sensitive and inherently personal private data subject to confidentiality laws.

97. In obtaining and storing Plaintiff's and Class Members' PII, Navigate360 owed a duty of reasonable care in safeguarding the PII.

98. Navigate360's networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PII were secured from unauthorized access.

99. Navigate360's networks, systems, protocols, policies, procedures and practices, as described above, were not reasonable given the sensitivity of the Plaintiff's and Class Members'

private data and the known vulnerabilities of Defendant's systems.

100. Navigate360 did not comply with federal laws and rules concerning the use and safekeeping of this private data.

101. Upon learning of the Data Breach, Navigate360 should have immediately disclosed the Data Breach to Plaintiff and Class Members, credit reporting agencies, the Internal Revenue Service, financial institutions and all other third parties with a right to know and the ability to mitigate harm to Plaintiff and Class Members as a result of the Data Breach.

102. Despite knowing its networks, systems, protocols, policies, procedures and practices, as described above, were not adequately designed, implemented, maintained, monitored and tested to ensure that Plaintiff's and Class Members' PII were secured from unauthorized access, Navigate360 ignored the inadequacies and was oblivious to the risk of unauthorized access it had created.

103. Despite knowing of the extreme sensitivity of Plaintiff's and Class Members' information and promising anonymity as a result, Defendant secretly tracked user behavior under the guise of security and stored PII and other information about tipsters.

104. Navigate360's behavior establishes facts evidencing a reckless disregard for Plaintiff's and Class Members' rights.

105. Navigate360, therefore, was grossly negligent.

106. The negligence is directly linked to injuries.

107. As a result of Navigate360's reckless disregard for Plaintiff's and Class Members' rights by failing to secure their PII, despite knowing its networks, systems, protocols, policies, procedures and practices were not adequately designed, implemented, maintained, monitored and tested, Plaintiff and Class Members suffered injury, which includes but is not limited to the exposure to a heightened, imminent risk of fraud, identity theft, financial and other harm. Plaintiff and Class Members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiff and Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit

freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and Class Members are also at increased risk of physical harm as a result of the Data Breach.

108. The harm to Plaintiff and the Class Members was a proximate, reasonably foreseeable result of Defendant's breaches of the applicable laws and regulations.

109. Therefore, Plaintiff and Class Members are entitled to damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

110. Plaintiff incorporates the foregoing allegations 1 to 69 as if fully set forth herein.

111. Plaintiff and Class Members were required to provide their PII, directly or indirectly, to obtain services from Navigate360. Plaintiff and Class Members entrusted their PII to Navigate360 in order to obtain services from them.

112. By providing their PII, and upon Navigate360's acceptance of such information, Plaintiff and Class Members on the one hand, and Navigate360 on the other hand, entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the services provided, whereby Navigate360 was obligated to take reasonable steps to secure and safeguard that information. Navigate360 on one hand and Plaintiff and class members on the other, further entered into an express contract for anonymity in exchange for furnishing information related to a crime.

113. Navigate360 had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with their contractual obligations. Navigate360 further had an express contractual duty to maintain Plaintiff and Class Members' anonymity.

114. Navigate360 was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class

Members' PII and to comply with industry standards and state laws and regulations for the security of this information, and Navigate360 expressly assented to these terms in its Privacy Policy as alleged above.

115. Under these implied contracts for data security, and express contracts for anonymity, Navigate360 was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

116. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Navigate360, including paying for the services provided by Navigate360 and/or providing the PII required by Navigate360.

117. Navigate360 breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach. Navigate360 breached express contracts by failing to keep Plaintiff and Class Members' identity anonymous. Navigate360 unreasonably interfered with the contract benefits owed to Plaintiff and Class Members.

118. Further, on information and belief, Navigate360 has not yet provided Data Breach notifications to affected Class Members who may already be victims of identity fraud or theft, or are at imminent risk of becoming victims of identity theft or fraud, associated with the PII that they provided to Navigate360. These Class Members are unaware of the potential source for the compromise of their PII.

119. The Data Breach was a reasonably foreseeable consequence of Navigate360's actions in breach of these contracts.

120. As a result of Navigate360's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value as compared to the secure services they were promised. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the secure services they were promised and the services they received.

121. Neither Plaintiff, nor Class Members, nor any reasonable person would have

provided their PII to Navigate360 had Navigate360 disclosed that its security was inadequate or that it did not adhere to industry-standard security measures.

122. As a result of Navigate360's breach, Plaintiff and Class Members have suffered actual damages resulting from theft of their PII, as well as the loss of control of their PII, and remain at imminent risk of suffering additional damages in the future.

123. As a result of Navigate360's breach, Plaintiff and the Class Members have suffered actual damages resulting from their attempt to mitigate the effect of the breach of implied contract and subsequent Data Breach, including, but not limited to, taking steps to protect themselves from the loss of their PII. As a result, Plaintiff and the Class Members have suffered actual identity theft and the ability to control their PII.

124. Accordingly, Plaintiff and Class Members have been injured as a result of Navigate360's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT

125. Plaintiff incorporates the foregoing allegations 1 to 69 as if fully set forth herein.

126. Plaintiff and the Class have stated claims against Defendant based on negligence, negligence per se, gross negligence, and violations of various federal statutes.

127. Defendant failed to fulfill its obligations to provide adequate and reasonable security measures for the PII of Plaintiff and the Class, as evidenced by the Data Breach.

128. As a result of the Data Breach, Defendant's system is more vulnerable to unauthorized access and requires more stringent measures to be taken to safeguard the PII of Plaintiff and the Class going forward.

129. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's current obligations to provide reasonable data security measures to protect the PII of Plaintiff and the Class. Defendant maintains that its security measures were—and still are—reasonably adequate and denies that it previously had or have any obligation to implement better

safeguards to protect the PII of Plaintiff and the Class.

130. Plaintiff seeks a declaration that Defendant must implement specific additional, prudent industry security practices to provide reasonable protection and security to the PII of Plaintiff and the Class. Specifically, Plaintiff and the Class seek a declaration that Defendant's existing security measures do not comply with its obligations, and that Defendant must implement and maintain reasonable security measures on behalf of Plaintiff and the Class to comply with its data security obligations.

VII. PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

DATED: March 31, 2026

Respectfully submitted,

/s Thomas D. Warren

WARREN TERZIAN LLP
Thomas D. Warren (0077541)
30799 Pinetree Rd., Suite 345
Pepper Pike, OH 44124
Tel: (216) 304-4970
tom.warren@warrenterzian.com

COTCHETT PITRE & McCARTHY LLP
Thomas E. Loeser (*pro hac vice to be filed*)
Ellen J Wen (*pro hac vice to be filed*)
1809 7th Ave., Ste. 1610
Seattle, WA 98101
Tel: (206) 802-1272
Fax: (206) 299-4184
tloeser@cpmlegal.com
ewen@cpmlegal.com

Attorneys for Plaintiff and Proposed Class