IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

MALCOLM SCOTT and HELEN PROBST SCOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. STATE FARM MUTUAL AUTOMOBILE INSURANCE COMPANY, Defendant.	Case No. _____ **Removed from McLean County Circuit Court;** **Case No. 2023LA000114**

NOTICE OF REMOVAL

Defendant State Farm Mutual Automobile Insurance Company ("State Farm"), by and through its attorneys, and pursuant to 28 U.S.C §§ 1332, 1441, 1446, and 1453, brings this Notice of Removal ("Notice") to the United States District Court for the Central District of Illinois.

PLEASE TAKE NOTICE that State Farm hereby removes the above-captioned action, Case No. 2023LA000114, from the Circuit Court of the Eleventh Judicial Circuit, McLean County, Illinois to the United States District Court for the Central District of Illinois. State Farm provides the following "short and plain statement of the grounds for removal." 28 U.S.C. § 1446(a); *see also Dart Cherokee Basin Operating Co. v. Owens*, 574 U.S. 81, 87, 89 (2014).

1. On September 13, 2023, Plaintiffs Malcolm Scott and Helen Probst Scott ("Plaintiffs") filed a putative class action complaint in the Circuit Court of McLean County, Illinois. Compl. at 1, attached hereto as Exhibit 1. Plaintiffs bring claims against State Farm for (1) negligence, (2) negligence per se, (3) invasion of privacy (intrusion upon seclusion), (4) breach of fiduciary duty, (5) breach of implied contract, (6) unjust enrichment, (7) declaratory relief, and (8) violations of the Illinois Uniform Deceptive Trade Practices Act. *Id.* ¶¶ 65–124.

2. This Court has original subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA") because (1) there is minimal diversity of citizenship between Plaintiffs and Defendant, (2) there are more than 100 putative class members, (3) the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs, and (4) none of CAFA's exceptions apply, *see* 28 U.S.C. § 1332(d).

3. State Farm has also complied with all other removal requirements. So, removal to this Court is proper under 28 U.S.C. § 1441.

I. BACKGROUND.

4. Plaintiffs contend that on or around August 25, 2023, "malicious, unauthorized third parties" hacked State Farm's systems and accessed 400 million records containing "highly sensitive Personal Information." Compl. ¶ 1. According to Plaintiffs, this alleged data breach was "a direct and proximate result of" State Farm's purported failures to implement "adequate systems and procedures for maintaining, safeguarding, and protecting" customer information. *Id.* ¶¶ 4, 54–57. Plaintiffs further assert that State Farm has failed to "provide timely, accurate, and adequate notice" of the alleged breach to customers. *Id.* ¶ 57.

5. Based on those allegations, the Complaint asserts eight claims on behalf of two putative classes: (1) negligence, (2) negligence per se, (3) invasion of privacy (intrusion upon seclusion), (4) breach of fiduciary duty, (5) breach of implied contract, (6) unjust enrichment, (7) declaratory relief, and (8) violations of the Illinois Uniform Deceptive Trade Practices Act. *Id.* ¶¶ 58, 65–124. Plaintiffs also seek several forms of relief on behalf of themselves and the putative classes, including actual damages, punitive damages, injunctive relief, and costs and attorney's fees. *Id*. at 31.

6. State Farm denies the allegations in the Complaint, which are factually and legally baseless. The sole issue presented here is whether removal is proper based on the Court's original subject-matter jurisdiction under 28 U.S.C. § 1332(d).

II. REMOVAL IS TIMELY.

7. Plaintiffs served State Farm with the summons and Complaint on September 18,

2023. Affidavit of Service of Process, attached hereto as Exhibit 3. No additional pleadings have been filed in the State Court Action.

8. Because State Farm filed this Notice of Removal ("Notice") within 30 days of service, removal is timely. *See* 28 U.S.C. § 1446(b)(1).

III. VENUE IS PROPER.

9. Plaintiffs filed the State Court Action in McLean County, Illinois. Compl. at 1. So, the United States District Court for the Central District of Illinois is the proper venue. *See* 28 U.S.C. §§ 93(a)(1), 1391.

IV. THIS COURT HAS ORIGINAL JURISDICTION UNDER CAFA.

10. The Court has original subject-matter jurisdiction under CAFA because of the putative class size, the amount of damages Plaintiffs' Complaint puts in controversy, and the parties' diversity. CAFA provides that "[t]he district courts shall have original jurisdiction of any civil action in which the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, and is a class action in which . . . any member of a class of plaintiffs is a citizen of a State different from any defendant." 28 U.S.C. § 1332(d)(2). Section 1332(d)(5) also provides that CAFA jurisdiction extends to class actions in which there are at least 100 putative class members. *See* 28 U.S.C. § 1332(d)(5)(B). This case satisfies those requirements.

A. This is a class action with more than 100 putative class members.

11. Under CAFA, a "class action" is "any civil action filed under rule 23 of the Federal Rules of Civil Procedure or similar State statute or rule of judicial procedure authorizing an action to be brought by 1 or more representative persons as a class action." 28 U.S.C. § 1332(d)(1)(B). Plaintiffs allege they "bring this action on behalf of themselves and the following classes:

> **Nationwide Class:** All residents of the United States whose Personal Information was compromised as a result of the Data Breach.
>
> **Florida Subclass:** All residents of Florida whose Personal Information was compromised as a result of the Data Breach.

Compl. ¶ 58. Plaintiffs also seek to certify the State Court Action "as a class action pursuant to 735 Ill. Comp. Stat. Ann. 5/2-801-802". *Id.* at 31. Accordingly, this case fits CAFA's definition of a putative class action. *See* 28 U.S.C. § 1332(d)(1)(B).

12. Plaintiffs also allege that the above-mentioned classes contain "thousands, if not millions, of members." Compl. ¶ 59. Therefore, Plaintiffs' own allegations indicate that there are more than 100 putative class members, which satisfies CAFA's class size requirement.

B. The amount in controversy exceeds $5 million.

13. The "matter in controversy" also exceeds $5 million, exclusive of interest and costs. *See* 28 U.S.C. § 1332(d)(2). To determine the jurisdictional minimum, "[t]he question is not what damages the plaintiff will recover, but what amount is 'in controversy' between the parties." *Brill v. Countrywide Home Loans, Inc.*, 427 F.3d 446, 448 (7th Cir. 2005). "That the plaintiff may fail in its proof, and the judgment be less than the threshold (indeed, a good chance that the plaintiff will fail and the judgment will be zero) does not prevent removal." *Id.*

14. Because the Complaint does not state an amount in controversy, this Notice need only contain "a plausible allegation that the amount in controversy exceeds the jurisdictional threshold." *Dart*, 574 U.S. at 89. "[T]he defendant's amount-in-controversy allegation should be accepted when not contested by the plaintiff or questioned by the court." *Id.* at 87; *see also Roppo v. Travelers Com. Ins. Co.*, 869 F.3d 568, 578–79 (7th Cir. 2017). So, a defendant does not need to make "evidentiary submissions" to establish the amount in controversy under CAFA. *Dart*, 574 U.S. at 84.

15. Here, Plaintiffs—on behalf of themselves and the putative classes—seek "actual and statutory damages, punitive damages, nominal damages, and monetary damages to the maximum extent allowable." Compl. at 31. Plaintiffs also seek attorney's fees, costs, expenses, pre- and post-judgment interest, and declaratory and injunctive relief. *Id.*[1] Courts may consider the value for each of those requests for relief when determining whether Plaintiffs' claims satisfy

[1] State Farm denies Plaintiffs or any putative class members are entitled to any form of damages or any relief whatsoever. The following calculations and amounts are for purposes of removal only.

CAFA's amount-in-controversy requirement. *Daley v. Jones Motor Co.*, 743 F. App'x 35, 37 (7th Cir. 2018) (holding the amount-in-controversy requirement met because, "theoretically," the compensatory and punitive damages could total more than $5 million); *see America's Money Line, Inc. v. Coleman*, 360 F.3d 782, 786 (7th Cir. 2004) ("In suits seeking the equitable remedies of an injunction or a declaratory judgment, the amount in controversy is determined by the value to the plaintiff (or petitioner) of the object of the litigation."); *Oshana v. Coca-Cola Co.*, 472 F.3d 506, 512 (7th Cir. 2006) (holding attorneys' fees and costs count towards CAFA's requirement).

16. State Farm designed and conducted a search of its Enterprise Financial Operations – Financial and Regulatory Reporting System to identify the total number of insurance policies that State Farm had in force as of September 30, 2023. That system query resulted in 50,022,859 policies. Owen Declaration ¶ 4, attached hereto as Exhibit 4. Even if some customers had multiple entries—*e.g.*, a customer had more than one insurance policy—a conservative extrapolation from that data is 25,011,429 customers with records affected by the alleged data breach.

17. Plaintiffs contend that consumers place "considerable" value on data privacy and that, as a result of the alleged breach, customers have suffered damages including, among other things, loss of "the full monetary value" of their transactions with State Farm. Compl. ¶¶ 44–45. Moreover, Plaintiffs request that State Farm be "compelled to provide for the benefit of Plaintiffs and [putative] class members all unlawful proceeds [it] received . . . as a result of the conduct and Data Breach alleged." *Id.* ¶ 111. Even assuming the monetary value of each putative class member's transaction is $1, an amount certainly less than "considerable," *id.* ¶ 44, the amount in controversy exceeds $5 million (25,011,429 record holders x $1 = $25,011,429).

18. Thus, CAFA's amount-in-controversy requirement is satisfied based on Plaintiffs' allegations that each putative class member has been deprived of the full value of their transactions with State Farm. *See* Compl. ¶ 45.

19. Even if the purported amount of actual damages for each putative class member was much lower than $1, CAFA's amount-in-controversy requirement is still satisfied because Plaintiffs also seek punitive damages, Compl. at 31. Punitive damages are potentially available for

intentional torts, such as Plaintiffs' invasion-of-privacy claim, should Plaintiffs prove their claims (which they cannot). *Ainsworth v. Century Supply Co.*, 693 N.E.2d 510, 514–15 (Ill. App. 1998). Illinois courts have approved punitive damage awards of three times the actual damages. *Daley*, 743 F. App'x at 37. So, to reach CAFA's $5 million threshold, the actual damages would only need to be $0.05 for each putative class member, conservatively assuming there are 25,011,429 unique policy holders for purposes of this removal.[2]

20. Further, based on Plaintiffs' allegation that each affected customer experienced a loss of the full value of their transactions with State Farm and their request for punitive damages, there would need to be only 1,250,000 putative class members to satisfy the amount-in-controversy requirement.[3]

21. Plaintiffs' request for injunctive relief is further evidence that CAFA's amount-in-controversy requirement is satisfied. Courts consider "what compliance with an injunction would cost the defendant" when evaluating the amount in controversy. *Roppo*, 869 F.3d at 580. Plaintiffs don't explain what an injunction here would include. *See* Compl. at 31 (seeking to enjoin "State Farm from continuing the unlawful practices as set forth above"). But complying with an injunction that prevents State Farm from conducting all the actions that Plaintiffs complain of would be a significant cost.

22. Finally, Plaintiffs also seek attorneys' fees and costs. *Id*. While State Farm cannot assess what those fees and costs may be, any amount would just cement its good-faith estimate that Plaintiffs' claims meet CAFA's amount-in-controversy requirement. *See Oshana*, 472 F.3d at 512 (holding attorneys' fees count towards CAFA's requirement); *ABM Sec. Servs. v. Davis*, 646

[2] Here are State Farm's calculations of theoretical damages:
- $0.05 (actual damages) x 3 = $0.15 (potential punitive damages award)
- $0.05 + $0.15 = $0.20 (total damages per putative class member)
- $0.20 x 25,011,429 = $5,002,285.80 (plausible aggregate damages for putative class)

[3] Here are State Farm's calculations to arrive at 1,250,000 putative class members:
- $1 (actual damages) x 3 = $3 (potential punitive damages award)
- $1 + $3 = $4 (total damages per putative class member)
- $5 million (CAFA's requirement) ÷ $4 = 1,250,000 (putative class members)

F.3d 475, 479 (7th Cir. 2011) (reversing district court's remand of putative class action, in part, because "[t]he district court also failed to satisfactorily explain why it was legally impossible for there to be at least $5,552 in attorneys' fees in controversy at the time of removal").

23. Because each putative class member would only need to recover a nominal amount in actual damages, it would cost State Farm significant amounts to comply with any injunction, and Plaintiffs have incurred attorneys' costs and fees, State Farm has shown the amount in controversy plausibly exceeds $5 million.

C. Minimal diversity exists.

24. There is also minimal diversity under CAFA because at least one Plaintiff is a citizen of a different state from the Defendant. *See* 28 U.S.C. § 1332(d)(2)(a).

25. Plaintiffs allege they are citizens of Florida. Compl. ¶¶ 13, 16.

26. Defendant State Farm is a citizen of Illinois because it is an "Illinois corporation, with its principal place of business in Bloomington, Illinois." *Id.* ¶ 19; *see* 28 U.S.C. § 1332(c)(1); *Hart v. FedEx Ground Package Sys. Inc.*, 457 F.3d 675, 676 (7th Cir. 2006) (holding that "it has been established that the grant of diversity jurisdiction in Article III of the Constitution permits the federal courts to decide cases with only 'minimal' diversity—that is, just one party with citizenship different from all others—and that the 'complete' diversity requirement is statutory").

27. Because Plaintiffs are, allegedly, citizens of Florida and Defendant State Farm is a citizen of Illinois, minimal diversity exists. *See* 28 U.S.C. § 1332(d)(2)(a).

D. None of CAFA's exceptions apply.

28. Neither the discretionary home-state exception, nor the local-controversy exception applies here. *See* 28 U.S.C. § 1332(d)(3)–(4).[4] Those exceptions require a certain portion of the putative class to be citizens of the state where Plaintiffs originally sued—*i.e.*, Illinois. *See* 28 U.S.C. § 1332(d)(4)(A)(i) (local-controversy exception, requiring federal courts to decline

[4] While no CAFA exception applies here, the burden would be on Plaintiffs to prove that one does. *Breuer v. Jim's Concrete of Brevard, Inc.*, 538 U.S. 691, 698 (2003); *Hart*, 457 F.3d at 680 ("[T]he party seeking to take advantage of the home-state or local exception to CAFA jurisdiction has the burden of showing that it applies.").

jurisdiction when greater than two-thirds of the members of all proposed plaintiff classes in the aggregate are citizens of the State in which the action was originally filed); 28 U.S.C. § 1332(d)(4)(B) (mandatory home-state exception, requiring federal courts to decline jurisdiction when "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State in which the action was originally filed"); 28 U.S.C. § 1332(d)(3) (discretionary home-state exception, providing that a district court *may* decline to exercise jurisdiction "over a class action in which greater than one-third but less than two-thirds of the members of all proposed plaintiff classes in the aggregate and the primary defendants are citizens of the State in which the action was originally filed").

29. The home-state and local-controversy exceptions do not apply because Plaintiffs cannot prove that the requisite portion of class members are citizens of Illinois. *First*, both putative classes here consist of ***residents*** of the United States and Florida. Compl. ¶ 58. But residency is not the same as ***citizenship***. *In re Sprint Nextel Corp.*, 593 F.3d 669, 671, 676 (7th Cir. 2010) (holding home-state exception did not apply because plaintiffs sought to represent a putative class of "all Kansas residents," not "Kansas *citizens*" (emphasis in original)); *Norman v. Campbell*, 87 F. App'x 582, 585 (7th Cir. 2003) ("Norman, though, actually focuses on the ***residency***, not the ***citizenship***, of the parties, but allegations of residency cannot invoke the diversity jurisdiction." (emphasis added)); *Smith v. Marcus & Millichap, Inc.*, 991 F.3d 1145, 1157 (11th Cir. 2021) (denying plaintiff's motion to remand based on local-controversy exception because "[i]n cases where plaintiffs do not base citizenship on the class definition, they must provide evidence of the class members' state of residence as well as evidence showing their intent to remain in that state"). The Complaint shows Plaintiffs understand that distinction because they allege to be Florida citizens. *See* Compl. ¶¶ 13, 16.

30. Because the putative classes are defined by residency, rather than citizenship, neither the home-state nor the local-controversy exception applies. *Smith*, 991 F.3d at 1157.

31. *Second*, even assuming residency is the same as citizenship, which it is not, Plaintiffs have not pled facts demonstrating that any putative class members are residents of

Illinois. *See* Compl. ¶ 58. Thus, Plaintiffs fail to show that more than one-third or more than two-thirds of putative class members are citizens of the state in which the suit was filed, as respectively required by the home-state and local-controversy exceptions. *See* 28 U.S.C. § 1332(d)(4)(A)(i); 28 U.S.C. § 1332(d)(4)(B); 28 U.S.C. § 1332(d)(3).

V. STATE FARM HAS SATISFIED ALL OTHER REQUIREMENTS.

32. State Farm has also satisfied all other requirements for removal under 28 U.S.C. § 1446.

33. ***Process, pleadings, and orders.*** 28 U.S.C. § 1446(a) requires State Farm to provide this Court with a copy of all "process, pleadings, and orders" served on it in the state court action. As noted above, State Farm has attached true and correct copies of these documents:

- Class Action Complaint (Exhibit 1)
- Summons as to State Farm (Exhibit 2)
- Affidavit of Service of Process as to State Farm (Exhibit 3)

34. ***Notice to adverse parties and state court.*** Per 28 U.S.C. § 1446(d), State Farm will promptly serve copies of this Notice on Plaintiffs' counsel and will file the Notice with the clerk for the Circuit Court of the Eleventh Judicial Circuit, McLean County, Illinois. State Farm will also separately file with this Court the required "Notice to the Plaintiff."

35. ***Other matters*.** If Plaintiffs oppose removal, State Farm asks for the opportunity to submit briefing, argument, and additional evidence to show why removal is proper. State Farm also reserves the right to amend or supplement this Notice. By filing this Notice, State Farm does not waive or relinquish its right to assert any defense or objection to the complaint's merits or class treatment.

VII. CONCLUSION.

The Court has subject-matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332, and removal is proper under 28 U.S.C. §§ 1441 and 1446.

Dated: October 18, 2023

Respectfully submitted,

s/ John P. Heil, Jr.

John P. Heil, Jr. (IL ARDC #6237286)
Jessica A. Pullen (IL ARDC #6342509)
HEYL, ROYSTER, VOELKER & ALLEN, PC
300 Hamilton Boulevard, P.O. Box 6199
Peoria, IL 61601-6199
Tel.: 309-676-0400
Fax: 309-676-3374
jheil@heylroyster.com
jpullen@heylroyster.com

Cari K. Dawson (*Court admission pending*)
Daniella Main (*Court admission pending*)
ALSTON & BIRD LLP
One Atlantic Center
1201 W Peachtree St NE, Suite 4900
Atlanta, GA 30309
Tel.: 404-881-7000
cari.dawson@alston.com
daniella.main@alston.com

Attorneys for Defendant State Farm Mutual Automobile Insurance Co.

CERTIFICATE OF SERVICE

I certify that on October18, 2023, I electronically filed this Notice of Removal and supporting exhibits with the Clerk of the Court by using the Court's CM/ECF system, which will send notification to all counsel of record.

s/ John P. Heil, Jr.
John P. Heil, Jr.
HEYL, ROYSTER, VOELKER & ALLEN, PC
300 Hamilton Boulevard, P.O. Box 6199
Peoria, Illinois 61602
Tel.: 309-676-0400
Fax: 309-676-3374

Attorney for Defendant

EXHIBIT 1

IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT
MCLEAN COUNTY, ILLINOIS

MALCOLM SCOTT and HELEN PROBST SCOTT, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

STATE FARM MUTUAL AUTOMOBILE INSURANCE COMPANY,

Defendant.

Case No. 2023LA000114

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

FIRST CASE MANAGEMENT CONFERENCE
BEFORE JUDGE FOLEY
SET ON 03/06/2024 AT 9:00 AM

Plaintiffs Malcolm Scott and Helen Probst Scott ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, bring this Class Action Complaint against Defendant State Farm Mutual Automobile Insurance Company ("State Farm" or "Defendant"), and in support thereof allege as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("class members"), whose highly sensitive Personal Information was amongst the 400 million records accessed and hacked by malicious, unauthorized third parties that removed the Personal Information from systems used by State Farm as early as August 25, 2023[1] (the "Data Breach").

2. State Farm describes itself as the "leading Auto and Home insurer in the United States."[2] It is the parent company of numerous subsidiaries, including entities spanning across

[1] DrinkMoreCodeMore, REDDIT (Sep. 2, 2023), https://www.reddit.com/r/cybersecurity/comments/168alg5/state_farm_claimed_as_a_victim_by_both_ransomed/; *see also infra* ¶¶ 33-34.
[2] STATE FARM, *2022 Annual Report*, https://www.statefarm.com/content/dam/sf-library/en-us/secure/legacy/pdf/2022-annual-report.pdf (last accessed Sep. 7, 2023).

every facet of the insurance industry, as well as a substantial presence in the banking, investment, and finance industries.[3]

3. State Farm touts the safety and security of its services on its website, www.statefarm.com. For instance, State Farm's website states: [4]

> We maintain physical, electronic, and procedural safeguards to protect customer information and to comply with federal and state laws. In addition, we review our policies and practices, monitor our computer networks, and test the strength of our security.

4. Contrary to its assurances to consumers, however, State Farm lacked adequate systems and procedures for maintaining, safeguarding, and protecting highly sensitive Personal Information entrusted to it. Specifically, on or about August 28, 2023, ransomware hackers announced that they had stolen 400 million records from State Farm's systems.[5] In the ordinary course of its business, State Farm obtains possession of (and stores) individuals'—including Plaintiffs' and class members'—highly sensitive Personal Information, which ordinarily includes: (1) full names, (2) mailing and billing addresses, (3) phone numbers, (4) email addresses, (5) dates of birth, (6) Social Security numbers, (7) driver's license numbers and/or other government-issued identification numbers, (8) bank account numbers and/or credit/debit card numbers, expiration dates, and CVV numbers, (9) automobile and health insurance information (such as insurance companies, member numbers, Medicaid-Medicare ID numbers, payer name, payer contract dates, policy information including type and deductible amount and subscriber number), (10) patient demographic information, (11) medical and/or treatment information (dates of service, location,

[3] STATE FARM, *Company Overview*, https://www.statefarm.com/about-us/company-overview (last accessed Sep. 7, 2023).
[4] STATE FARM, *Notice of Privacy Policy*, https://www.statefarm.com/customer-care/privacy-security/privacy#accordion-f8ae9e451f-item-be4000d59c (last accessed Sep. 7, 2023).
[5] *See supra* n.1.

services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); (12) billing and/or claims information (invoices, submitted claims and appeals, and patient account identifiers used by the provider); and (13) information of any parent, guardian, or guarantor (collectively, "Personal Information"). State Farm stores this information digitally in the regular course of business.

5. Despite this Data Breach being publicized over a week ago, State Farm still has not notified affected consumers—including Plaintiffs and class members—that their data may be in the hands of cyber criminals.

6. State Farm owed duties to Plaintiffs and class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Personal Information against unauthorized access and disclosure.

7. State Farm could have prevented the Data Breach by properly vetting and monitoring their systems.

8. Plaintiffs and class members entrusted State Farm with, and allowed State Farm to gather, highly sensitive information relating to their health and other matters as part of seeking medical treatment. They did so in confidence, and they had the legitimate expectation that State Farm would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

9. Trust and confidence are key components of Plaintiffs' and class members' relationship with State Farm. Without it, Plaintiffs and class members would not have provided State Farm with, or allowed State Farm to collect, their most sensitive information in the first place.

To be sure, Plaintiffs and class members relied upon State Farm to keep their information secure, as it is required by law to do.

10. State Farm breached its duties to class members by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the Personal Information entrusted to it from unauthorized access and disclosure.

11. As a result of State Farm's breach of its duties and obligations, the Data Breach occurred and Plaintiffs' and class members' Personal Information was accessed by, and disclosed to, an unauthorized third-party actor. This instant action seeks to remedy State Farm's failings and their consequences. Plaintiffs thus bring this complaint on behalf of themselves and all similarly situated individuals whose Personal Information was exposed as a result of the Data Breach.

12. Plaintiffs, on behalf of themselves and all other class members, assert claims for negligence; negligence per se; invasion of privacy; unjust enrichment; and violations of Illinois Uniform Deceptive Trade Practices Act ("IUDTPA"), 815 Ill. Comp. Stat. Ann. 510/1, *et. al.*, and seeks declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiff Malcolm Scott

13. Plaintiff Malcolm Scott is a resident and citizen of Florida and resides in Riverview, Florida.

14. Plaintiff Malcolm Scott jointly holds a Florida automobile insurance policy procured through State Farm with his wife, Plaintiff Helen Probst Scott, with an effective date of October 26, 2023. Plaintiff has been insured through State Farm since 1997.

15. Prior to retaining counsel for claims related to the Data Breach, Plaintiff Malcolm

Scott spent time monitoring his account for fraudulent activity and identity theft. He will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

B. Plaintiff Helen Probst Scott

16. Plaintiff Helen Probst Scott is a resident and citizen of Florida and resides in Riverview, Florida.

17. Plaintiff Helen Probst Scott jointly holds a Florida automobile insurance policy procured through State Farm with her husband, Plaintiff Malcolm Scott, with an effective date of October 26, 2023. Plaintiff has been insured through State Farm since 1997.

18. Prior to retaining counsel for claims related to the Data Breach, Plaintiff Helen Probst Scott spent time monitoring her account for fraudulent activity and identity theft. She will continue to expend further time doing so in the days, weeks, and months following the filing of this complaint.

C. Defendant

19. Defendant State Farm Mutual Automobile Insurance Company is an Illinois corporation, with its principal place of business in Bloomington, Illinois.

JURISDICTION AND VENUE

20. The Court has general personal jurisdiction over Defendant State Farm pursuant to 735 Ill. Comp. Stat. Ann. 5/2-209(b)(3)-(4) because State Farm maintains its headquarters and principal place of business in this County (i.e., in Bloomington, Illinois) and conducts substantial business in Illinois.

21. This Court is the proper venue for this case pursuant to 735 Ill. Comp. Stat. Ann. 5/2-101 because a substantial part of the events and omissions giving rise to Plaintiffs' claims

occurred in this County, Defendant State Farm maintains physical offices and principal places of business in this County, and because Defendant State Farm conducts a substantial part of its business within this County.

FACTUAL ALLEGATIONS

A. Overview of Defendant

22. State Farm's website assures consumers—such as Plaintiffs and class members—that "State Farm is dedicated to maintaining the confidentiality, integrity and availability of State Farm systems and information. We care about protecting our customers and associates from the security risks of everyday life."[6]

23. Likewise, State Farm touts the security of its services as follows:

> **We Protect Customer Information**
>
> We maintain physical, electronic, and procedural safeguards to protect customer information and to comply with federal and state laws. In addition, we review our policies and practices, monitor our computer networks, and test the strength of our security.[7]

24. These supposed "physical, electronic, and procedural" safeguards include "Knowledge Based Authentication," and partnership with a specialized verification provider that can "keep [consumer] information safer from those who might want to illegally access it or use it for fraudulent purposes."[8]

---

[6] STATE FARM, *Securing your personal information is a State Farm® priority*, https://www.statefarm.com/customer-care/privacy-security/security#accordion-0d3dedc429-item-4323a41e6b (last accessed Sep. 7, 2023).
[7] STATE FARM, *Notice of Privacy Policy*, https://www.statefarm.com/customer-care/privacy-security/privacy#accordion-f8ae9e451f-item-be4000d59c (last accessed Sep. 7, 2023).
[8] STATE FARM, *Securing your personal information is a State Farm® priority*, https://www.statefarm.com/customer-care/privacy-security/security#accordion-0d3dedc429-item-4323a41e6b (last accessed Sep. 7, 2023).

25. State Farm specifically lists the types of data vulnerabilities these supposed security measures aim to protect against, including "'Denial of Service' attack[s] of any kind," individuals "accessing or modifying data in an account that does not belong to [them]," "phishing," and "malicious software or security tools."[9]

26. Additionally, State Farm's website represents State Farm as an expert in cyber privacy, offering insurance coverage for cyber attacks, cyber extortion, and identity theft.[10]

27. State Farm even publishes articles providing specific advice on how to guard against cyber criminals. In some of these articles, State Farm advises companies to "put safety guardrails in place to protect your small business data," asserting the importance of "understand[ing] how cyber thieves work."[11] In others, State Farm offers guidance on how to "protect [one]self from data breaches."[12]

28. State Farm also advertises its partnership with Illinois State University, through which the University "launched a cybersecurity major" and "establish[ed] the Cybersecurity Center on campus, providing laboratory workspace and student collaboration areas for students in the School of Information Technology."[13]

29. Based on the foregoing, State Farm was aware that it owed duties to Plaintiffs and

---

[9] STATE FARM, *Vulnerability Disclosure Policy*, https://www.statefarm.com/customer-care/privacy-security/security/vulnerability-disclosure-policy (last accessed Sep. 7, 2023).
[10] STATE FARM, *Identity Restoration*, https://www.statefarm.com/insurance/identity-restoration (last accessed Sep. 7, 2023).
[11] STATE FARM, *Security and cyber security for small businesses* (May 23, 2023), https://www.statefarm.com/simple-insights/small-business/security-and-cybersecurity-tips-for-small-businesses.
[12] STATE FARM, *How to help protect yourself from data breaches*, https://www.statefarm.com/simple-insights/residence/how-to-help-protect-yourself-from-data-breaches (last accessed Sep. 7, 2023).
[13] STATE FARM, *Investing in the Cybersecurity Workforce of the Future* (April 27, 2021), https://newsroom. statefarm.com/investing-in-the-cybersecurity-workforce-of-the-future/

class members to keep their Personal Information safe and secure, which includes duties to ensure that all information State Farm collects, stores and/or transfers is secure, and that State Farm maintained adequate and commercially reasonable data security practices to ensure the protection of Personal Information within State Farm's possession, as well as duties to notify consumers affected by any breach in a timely fashion.

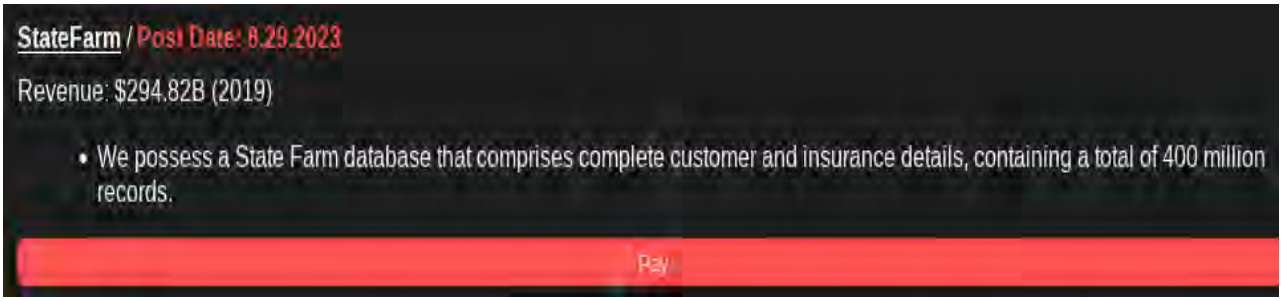
30. Discovery will show that through State Farm's provision of its services, it obtains possession of individuals'—including Plaintiffs' and class members'—highly sensitive Personal Information and stores or otherwise maintains it in the regular course of its businesses. Yet, contrary to State Farm's website representations, State Farm did not have adequate measures in place to protect and maintain sensitive Personal Information entrusted to it.

B. The Data Breach

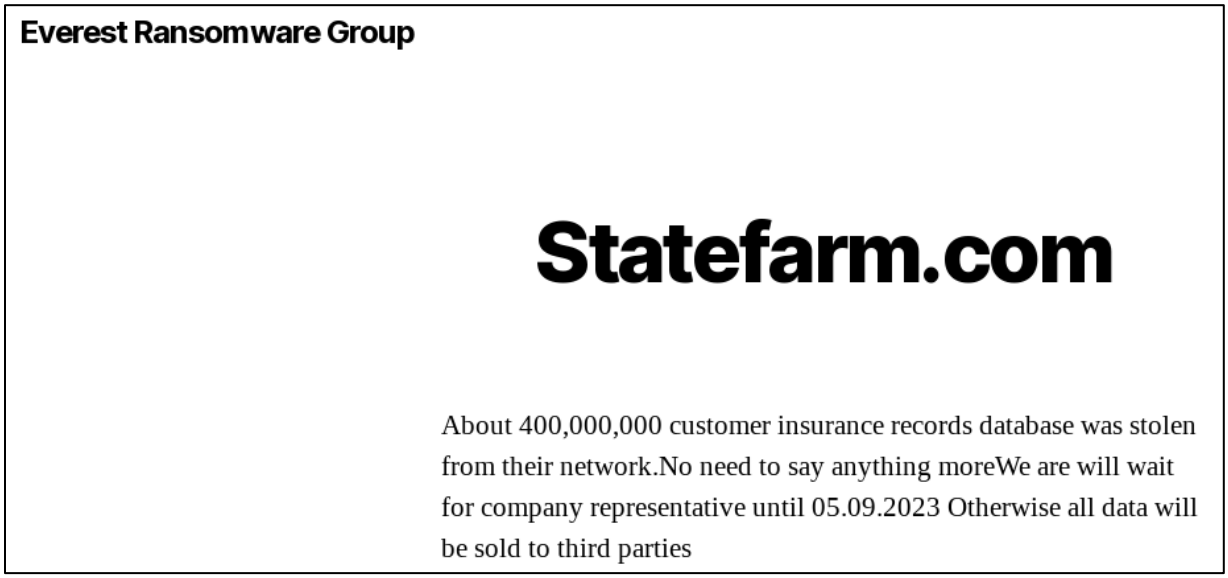
31. Two ransomware hacking groups have claimed responsibility for the data breach: Ransomed.vc ("Ransomed") and the Everest Ransomware Group ("Everest").[14] News agencies specializing in monitoring the activities of dark web criminals have reported that these two hacking groups are frequent collaborators, with overlapping leadership.[15]

32. On August 29, 2023, Everest and Ransomed posted about their successful breach of State Farm's data storage security, claiming to possess a data that comprises "complete customer and insurance details, containing a total of 400 million records":

[14] *See supra* n.1.
[15] *See* SOCRADAR, *On the Horizon: Ransomed.vc Ransomware Group Spotted in the Wild* (Aug 21, 2023), https://socradar.io/on-the-horizon-ransomed-vc-ransomware-group-spotted-in-the-wild/.



33. Additionally, Everest and Ransomed posted on an online website that "[a]bout 400,000,000 customer insurance records database was stolen from [State Farm's] network" and that they "will wait for company representatives until 05.09.2023 Otherwise [sic] all data will be sold to third parties":



34. Everest and Ransomed's hacking attacks are responsible for major data breaches, including data thefts against major corporations and government entities such as Transunion,[16] AT&T,[17] and the United States National Aeronautics and Space Administration ("NASA").[18]

[16] *Id.*
[17] *See* CYBERNEWS, *Everest ransom group adds AT&T to its victim list* (Oct. 28, 2022), https://cybernews.com/news/att-hit-everest-ransomware/.
[18] *See* THE CYBER EXPRESS, *Everest Ransomware Group Targets NASA Partners* (May 2, 2022), https://thecyberexpress.com/everest-ransomware-group-puts-data-on-sale/.

35. In many cases, Everest and Ransomed sell the stolen data to anyone willing to pay for access.[19] In others, they simply make the data available online for anyone to download and view.[20]

36. Because the Data Breach was conducted by known, self-proclaimed ransomware cybercriminals, Plaintiffs' and class members' sensitive Personal Information are irrefutably in the possession of known bad actors. Additionally, based on Everest and Ransomed's statement above, Plaintiffs' and class members' Personal Information may have already been sold to criminal third parties, which places them at imminent risk that their data will be misused.

37. While the specific methodology used by Everest and Ransomed to access State Farm's database is currently unknown, past attacks by these hacking groups have generally involved "phishing" schemes, in which an email is sent to an employee of the target entity which, while appearing to be legitimate, is sent by a bad actor.

38. In such a phishing scheme, the data breach occurs when the employee clicks a link in the phishing email, executing malicious software which allows the hacker to access the entity's computer systems and databases.

39. As noted above, State Farm is well aware of the risk posed by phishing schemes.[21]

40. The Federal Trade Commission ("FTC") has published extensively on how businesses can prevent phishing schemes. Among its recommendations are implementing email

[19] FN 23; 25; 25, *supra*.
[20] *See* RESTORE PRIVACY, *Everest Ransomware Group Leaks MultiCare Medical Data in Latest Data Breach* (Oct. 17, 2022), https://restoreprivacy.com/everest-ransomware-multicare-medical-data-breach/.
[21] *See supra* ¶ 26.

authentication systems,[22] keeping security systems up-to-date,[23] and regularly training staff to recognize phishing schemes.[24] Had State Farm seriously intended to protect the consumer Personal Information in its possession, it could have done so.

C. Defendant Knew that Criminals Target Personal Information

41. At all relevant times, State Farm knew, or should have known, its clients'—such as Plaintiffs' and all other class members'— Personal Information was a target for malicious actors. Despite such knowledge, State Farm failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and class members' Personal Information from cyber-attacks that State Farm should have anticipated and guarded against.

42. Personal information is a valuable property right.[25] The value of Personal Information as a commodity is measurable.[26] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[27] American companies are estimated to have spent

[22] FEDERAL TRADE COMMISSION, *Businesses Can Help Stop Phishing and Protect their Brands Using Email Authentication* (Mar. 2017), https://www.ftc.gov/system/files/documents/reports/businesses-can-help-stop-phishing-protect-their-brands-using-email-authentication-ftc-staff/email_authentication_staff_perspective.pdf.
[23] FEDERAL TRADE COMMISSION, *Phishing*, https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/phishing (last accessed Sep. 7, 2023).
[24] *Id*.
[25] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[26] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[27] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

over $19 billion on acquiring personal data of consumers in 2018.[28] It is so valuable to identity thieves that once Personal Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

43. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers ("SSNs"), Personal Information and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

44. Consumers place a high value on the privacy of their Personal Information. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[29]

45. Given these facts, any company that transacts business with a consumer and then compromises the privacy of the consumer's Personal Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Theft of Personal Information Has Grave and Lasting Consequences for Victims

46. Theft of Personal Information is serious. The FTC warns consumers that identity

[28] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[29] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

thieves use Personal Information to exhaust financial accounts, start new utility accounts, and incur charges and credit in a person's name.[30]

47. Identity thieves use Personal Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[31] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that Personal Information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[32]

48. With access to an individual's Personal Information, 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; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the

---

[30] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 15, 2021).

[31] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

[32] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's Personal Information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[33]

49. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[34]

50. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

51. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other Personal Information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[35]

52. There may also be a time lag between when sensitive Personal Information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used

[33] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last accessed Nov. 15, 2021).
[34] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed Nov. 15, 2021).
[35] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

and it takes some individuals up to three years to learn that information.[36]

53. It is within this harsh and dangerous reality that Plaintiffs and all other class members must now live with the knowledge that their Personal Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

E. Damages and Harm Sustained by Plaintiffs and the Other Class Members

54. As a direct and proximate result of State Farm's failures alleged above, Plaintiffs and class members are at substantial risk of suffering identity theft and fraud or misuse of their Personal Information.

55. Plaintiffs and the Class suffered actual injury from having Personal Information compromised as a result of State Farm's negligent security processes and procedures and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Personal Information, a form of property that State Farm obtained from Plaintiffs and the Class; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

56. For the reasons mentioned above, State Farm's conduct, which directly and proximately caused the Data Breach, caused Plaintiffs and members of the Class these significant injuries and harm.

57. Plaintiffs bring this class action against State Farm for its failure to: (1) properly secure and safeguard Personal Information; (2) ensure that proper security measures were in place to protect Personal Information; and (3) provide timely, accurate, and adequate notice to Plaintiffs and other class members that their Personal Information had been compromised.

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

CLASS ALLEGATIONS

58. Plaintiffs bring this action on behalf of themselves and the following classes:

Nationwide Class: All residents of the United States whose Personal Information was compromised as a result of the Data Breach.

Florida Subclass: All residents of Florida whose Personal Information was compromised as a result of the Data Breach.

The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and its current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

59. **Numerosity**: Class members are so numerous that their individual joinder is impracticable, as the proposed Class includes—upon information and belief—thousands, if not millions, of members who are geographically dispersed.

60. **Typicality**: Plaintiffs' claims are typical of class members' claims. Plaintiffs and all class members were injured through State Farm's uniform misconduct, and Plaintiffs' claims are identical to the claims of the class members they seek to represent.

61. **Adequacy**: Plaintiffs' interests are aligned with the Class they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and undersigned counsel.

62. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other class members' claims. The injury suffered

by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress State Farm's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. 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 a single court.

63. **Commonality and Predominance:** The following questions common to all class members predominate over any potential questions affecting individual class members:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and class members' Personal Information from unauthorized access and disclosure;

b. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and class members' Personal Information;

c. Whether Defendant breached its duties to protect Plaintiffs' and class members' Personal Information;

d. Whether Defendant violated the statutes alleged herein;

e. Whether Plaintiffs and all other class members are entitled to damages and the measure of such damages and relief.

64. Given that Defendant engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

65. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

66. Defendant owed duties to Plaintiffs and all other class members to exercise reasonable care in safeguarding and protecting their Personal Information in Defendant's possession, custody, or control, including duties to safeguard that Personal Information. Defendant had an independent obligation to control all environments into which it placed consumers' Personal Information, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

67. Defendant owed duties to Plaintiffs and class members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and class members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

68. Defendant owed a duty of care to Plaintiffs and class members to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the Personal Information.

69. Defendant knew the risks of collecting and storing Plaintiffs' and all other class members' Personal Information and the importance of maintaining secure systems processes and

procedures in place to safeguard that Personal Information. Defendant knew of the many data breaches that targeted consumer Personal Information in recent years.

70. Given the nature of Defendant's businesses, the sensitivity and value of the Personal Information it maintains, and the resources at its disposal, Defendant should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

71. Defendant breached its duties in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and class members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

d. Failing to adequately monitor, evaluate, and ensure the security of its network and systems;

e. Failing to recognize in a timely manner that Plaintiffs' and class members' Personal Information had been compromised; and

f. Failing to timely and adequately disclose that Plaintiffs' and class members' Personal Information had been improperly acquired or accessed.

72. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and class members' Personal Information by failing to control, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols to ensure that all

software and hardware systems into which it placed consumers' data were protected against the unauthorized release, disclosure, and dissemination of Plaintiffs' and class members' Personal Information.

73. But for Defendant's negligent conduct or breach of the above-described duties owed to Plaintiffs and class members, their Personal Information would not have been compromised.

74. As a result of Defendant's above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other class members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their Personal Information permitted by Defendant; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

75. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

76. State Farm's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164,

Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

77. State Farm's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure Personal Information.

78. Defendant violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all other class members' Personal Information and not complying with applicable industry standards, including by failing to control all environments into which it placed consumers' Personal Information, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data. State Farm's conduct was particularly unreasonable given the nature and amount of Personal Information they obtain and store, and the foreseeable consequences of a data breach involving Personal Information including, specifically, the substantial damages that would result to Plaintiffs and the other class members.

79. State Farm's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence per se.

80. Plaintiffs and class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

81. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

82. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and class members' Personal Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and class members' Personal Information to unauthorized individuals.

83. The injury and harm that Plaintiffs and the other class members suffered was the direct and proximate result of State Farm's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiffs and class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their Personal Information permitted by Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT III
INVASION OF PRIVACY
(INTRUSION UPON SECLUSION)
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

84. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

85. Plaintiffs and class members had a reasonable expectation of privacy in the Personal Information that State Farm failed to safeguard and allowed to be accessed by way of the Data Breach.

86. State Farm's conduct as alleged above intruded upon Plaintiffs' and class members' seclusion under common law.

87. By intentionally and/or knowingly failing to keep Plaintiffs' and class members' Personal Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, State Farm intentionally invaded Plaintiffs' and class members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and class members' private affairs in a manner that identifies Plaintiffs and class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and class members.

88. State Farm knew that an ordinary person in Plaintiffs' and a class member's position would consider State Farm's intentional actions highly offensive and objectionable.

89. State Farm invaded Plaintiffs' and class members' right to privacy and intruded into Plaintiffs' and class members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their Personal Information without their informed, voluntary, affirmative, and clear consent.

90. State Farm intentionally concealed from Plaintiffs and class members an incident that misused and/or disclosed their Personal Information without their informed, voluntary,

affirmative, and clear consent.

91. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and class members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. State Farm's conduct, amounting to a substantial and serious invasion of Plaintiffs' and class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider State Farm's intentional actions or inaction highly offensive and objectionable.

92. In failing to protect Plaintiffs' and class members' Personal Information, and in intentionally misusing and/or disclosing their Personal Information, State Farm acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and class members' rights to have such information kept confidential and private.

93. As a direct and proximate result of the foregoing conduct, Plaintiffs seek an award of damages on behalf of themselves and the Class.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

94. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

95. Plaintiffs and class members gave State Farm their Personal Information in confidence, believing that State Farm would protect that information. Plaintiffs and class members would not have provided State Farm with this information had they known it would not be adequately protected. State Farm's acceptance and storage of Plaintiffs' and class members' Personal Information created a fiduciary relationship between State Farm and Plaintiffs and class members. In light of this relationship, State Farm must act primarily for the benefit of people

whose Personal Information is provided to it, which includes safeguarding and protecting Plaintiffs' and class members' Personal Information.

96. State Farm has a fiduciary duty to act for the benefit of Plaintiffs and class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and class members' Personal Information, failing to comply with the data security guidelines set forth by relevant law, and otherwise failing to safeguard Plaintiffs' and class members' Personal Information that it collected.

97. As a direct and proximate result of State Farm's breaches of its fiduciary duties, Plaintiffs and class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of, or imminent threat of, identity theft; (ii) the compromise, publication, and theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Personal Information which remains in State Farm's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Personal Information compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

98. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

99. In connection with receiving insurance coverage or other services, Plaintiffs and all other class members entered into implied contracts with State Farm.

100. Pursuant to these implied contracts, Plaintiffs and class members paid money to State Farm, and provided State Farm with their Personal Information. In exchange, State Farm agreed to, among other things, and Plaintiffs and class members understood that State Farm would: (1) provide insurance services to Plaintiffs and class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and class members' Personal Information; and (3) protect Plaintiffs' and class members' Personal Information in compliance with federal and state laws and regulations and industry standards.

101. The protection of Personal Information was a material term of the implied contracts between Plaintiffs and class members, on the one hand, and State Farm, on the other hand. Indeed, as alleged above, State Farm recognized the importance of data security and the privacy of its customers' and serviced individuals' Personal Information on its website and in its Privacy Notice. Had Plaintiffs and class members known that State Farm would not adequately protect their Personal Information, they would not have entrusted their Personal Information to State Farm.

102. Plaintiffs and class members performed their obligations under the implied contract when they provided State Farm with their Personal Information and paid for services from State Farm.

103. State Farm breached its obligations under its implied contracts with Plaintiffs and class members in failing to implement and maintain reasonable security measures to protect and secure their Personal Information and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and class members' Personal Information in a manner that complies with applicable laws, regulations, and industry standards.

104. State Farm's breach of its obligations of its implied contracts with Plaintiffs and class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other

class members have suffered from the Data Breach.

105. Plaintiffs and all other class members were damaged by State Farm's breach of implied contracts because: (i) they paid—directly or through their healthcare providers, insurers, and/or state agencies—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Personal Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Personal Information has been breached; (v) they were deprived of the value of their Personal Information, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

106. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

107. Plaintiffs and class members have both a legal and equitable interest in their Personal Information that was collected by, stored by, and maintained by State Farm—thus conferring a benefit upon State Farm—that was ultimately compromised by the Data Breach.

108. State Farm accepted or had knowledge of the benefits conferred upon them by Plaintiffs and class members. State Farm also benefitted from the receipt of Plaintiffs' and class members' Personal Information.

109. As a result of State Farm's failure to safeguard and protect Personal Information, Plaintiffs and class members suffered actual damages.

110. State Farm should not be permitted to retain the benefit belonging to Plaintiffs and class members because State Farm failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

111. State Farm should be compelled to provide for the benefit of Plaintiffs and class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT VII
DECLARATORY RELIEF
(28 U.S.C. § 2201)
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

112. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

113. An actual controversy has arisen and exists between Plaintiffs and class members, on the one hand, and State Farm on the other hand, concerning the Data Breach and State Farm's failure to protect Plaintiffs' and class members' Personal Information, including with respect to the issue of whether State Farm took adequate measures to protect that information. Plaintiffs and the Class are entitled to judicial determination as to whether State Farm have performed and are adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and class members' Personal Information from unauthorized access, disclosure, and use.

114. A judicial determination of the rights and responsibilities of the parties regarding State Farm's privacy policies and whether they failed to adequately protect Personal Information is necessary and appropriate to determine with certainty the rights of Plaintiffs and the Class, and so that there is clarity between the parties as to State Farm's data security obligations with respect to Personal Information going forward, in view of the ongoing relationships between the parties.

COUNT VIII
VIOLATIONS OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT ("IUDTPA")
815 Ill. Comp. Stat. Ann. 510/1, *et. al.*
(On Behalf of Plaintiffs, the Nationwide Class and the Florida Subclass)

115. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

116. State Farm sells and performs services in the State of Illinois.

117. Plaintiffs, class members, and State Farm are "persons" as defined by the IUDTPA. 815 Ill. Comp. Stat. Ann. 510/1(5).

118. State Farm obtained Plaintiffs' and class members' Personal Information in connection with the services they perform and provide.

119. State Farm engaged in unfair or deceptive acts in violation of the IUDTPA by failing to implement and maintain reasonable security measures to protect and secure consumers' (such as Plaintiffs' and class members') Personal Information in a manner that complied with applicable laws, regulations, and industry standards, including by failing to control all environments into which it placed consumers' Personal Information, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

120. As alleged above, State Farm makes explicit statements to its customers that their Personal Information will remain private and secure.

121. The IUDTPA lists twelve instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 815 Ill. Comp. Stat. Ann. 510/2. State Farm's failure to adequately protect Plaintiffs' and class members' Personal Information while holding out that it would adequately protect the Personal Information falls under at least the following categories:

a. Represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that he or she does not have (815 Ill. Comp. Stat. Ann. 510/2(5);

b. Represents that goods or services are of a particular standard, quality, or grade or that goods are a particular style or model, if they are of another (815 Ill. Comp. Stat. Ann. 510/2(7);

c. Engages in any other conduct which similarly creates a likelihood of confusion or misunderstanding (815 Ill. Comp. Stat. Ann. 510/2(12).

122. Due to the Data Breach, Plaintiffs and class members have lost property in the form of their Personal Information. Further, State Farm's failure to adopt reasonable practices in protecting and safeguarding their customers' Personal Information will force Plaintiffs and class members to spend time or money to protect against identity theft. Plaintiffs and class members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for State Farm's practice of collecting and storing Personal Information without appropriate and reasonable safeguards to protect such information.

123. As a result of State Farm's violations of the IUDTPA, Plaintiffs and class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Personal Information; (iii) breach of the confidentiality of their Personal Information; (iv) deprivation of the value of their Personal Information, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their Personal Information permitted by State Farm; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (viii) overpayment for the services that were received without adequate data security.

124. Pursuant to 815 Ill. Comp. Stat. Ann. 510/2, Plaintiffs seeks actual damages, costs and reasonable attorney fees.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to 735 Ill. Comp. Stat. Ann. 5/2-801-802, and appoint Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

B. Award Plaintiffs and the Class actual and statutory damages, punitive damages, nominal damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that class members have an effective remedy, including enjoining State Farm from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: September 12, 2023

By: */s/ John Albanese*

John Albanese (SBN: 6308461)
Berger Montague PC
1229 Tyler Street NE, Suite 205

Minneapolis, MN 55413
Tel: 612-594-5997
Fax: 612-584-4470
Email: jalbanese@bm.net

E. Michelle Drake (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
Email: emdrake@bm.net

Mark B. DeSanto (*Pro Hac Vice* forthcoming)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
Email: mdesanto@bm.net

William "Billy" Peerce Howard (*Pro Hac Vice* forthcoming)
THE CONSUMER PROTECTION FIRM, PLLC
401 East Jackson Street, Suite 2340
Tampa, FL 33602
Tel: (813) 500-1500
Fax: (813) 435-2369
Email: Billy@TheConsumerProtectionFirm.com

Amanda J. Allen (*Pro Hac Vice* forthcoming)
THE CONSUMER PROTECTION FIRM, PLLC
401 East Jackson Street, Suite 2340
Tampa, FL 33602
Tel: (813) 500-1500
Fax: (813) 435-2369
Email: Amanda@TheConsumerProtectionFirm.com

Counsel for Plaintiffs

ClassAction.org
