

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

Jeffrey Ebert, on behalf of himself and on behalf of his **minor children M.E., E.E., and S.E.**, and **Jennifer Ebert**, on behalf of herself, and collectively on behalf of all others similarly situated,

Plaintiffs,

v.

PRGX Global, Inc.,

Defendant.

Case No. 1:23-CV-04233-TWT

CLASS ACTION SETTLEMENT AGREEMENT

This Settlement Agreement dated June 20, 2024, is made and entered into by and among Jeffrey Ebert, on behalf of himself and on behalf of his minor children M.E., E.E., and S.E., and Jennifer Ebert, on behalf of herself, and collectively on behalf of all others similarly situated, and PRGX Global, Inc. (“PRGX” or “Defendant”) (together, the “Parties”).

I. BACKGROUND

1. This litigation arises from a data security incident involving the personally identifiable information (“PII”) and protected health information (“PHI”) of Plaintiffs and the proposed Settlement Class.

2. On April 9, 2022, PRGX noticed that certain computer servers and systems storing Plaintiffs' and the Settlement Class's PII and PHI were inaccessible (the "Data Incident").

3. After an investigation, PRGX determined that an unknown actor accessed its systems between April 8, 2022, and April 9, 2022, and took or viewed certain files containing the PII/PHI of Plaintiffs and the Settlement Class.

4. The PII/PHI of approximately 13,231 individuals was potentially impacted in the Data Incident.

5. The types of PII/PHI potentially accessed or viewed during the Data Incident included: names; dates of birth; Social Security numbers; driver's license numbers; credit card information; financial account information; health insurance information; medical information; electronic signatures; employer assigned identification numbers; passport numbers; and online usernames and passwords.

6. After PRGX provided notice of the Data Incident in May 2023, Plaintiffs filed a class action lawsuit against PRGX on June 12, 2023, in the Superior Court of Cobb County, State of Georgia, which PRGX later removed to the United States District Court for the Northern District of Georgia (Atlanta Division), on September 9, 2023.

7. On October 9, 2023, Plaintiffs filed their First Amended Class Action Complaint, asserting the following causes of action against PRGX: (i) Negligence;

(ii) Negligence Per Se; (iii) Unjust Enrichment; (iv) Breach of Implied Contract; and (v) Declaratory Relief.

8. On October 23, 2023, PRGX filed a Motion to Dismiss Plaintiff's First Amended Class Action Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6), to which Plaintiffs timely responded in opposition thereto on November 6, 2023.

9. Prior to engaging in mediation, the Parties engaged in informal discovery and explored and discussed at length the factual and legal issues in the Action and related to the Data Incident.

10. On February 22, 2024, the Parties participated in a full-day mediation session with Hon. Wayne R. Andersen (Ret.) (the "Mediator"). Although a settlement was not reached at the mediation, progress was made. At the end of the mediation the mediator made a confidential Mediator's proposal which resulted in a settlement in principle.

11. The Parties did not discuss attorneys' fees, costs, and expenses prior to reaching an agreement as to the material terms of the relief for Settlement Class Members.

12. The Parties recognize the outcome of the Action and the claims asserted in the Action are uncertain, and that protracted litigation of this Action to final judgment would entail substantial cost, risk, and delay of benefits and relief for

Plaintiffs and all Settlement Class Members. Specifically, PRGX denies each and all of the claims and contentions alleged against it in the Action. PRGX denies all allegations of wrongdoing or liability as alleged, or which could be alleged, in the Action. Nonetheless, PRGX has concluded that further defense of the Action would be protracted and expensive, and that it is desirable that the Action be fully and finally settled in the manner and upon the terms and conditions set forth in this Settlement Agreement.

13. The Parties desire to compromise and settle all issues, claims, and allegations asserted in the Action, or those claims that could have been asserted in the Action based upon the Data Incident, by or on behalf of Plaintiff and the Settlement Class.

14. The Parties agree that the Settlement Agreement offers significant benefits to all Settlement Class Members and is fair, reasonable, adequate, and in the best interest of Plaintiffs and all Settlement Class Members.

15. This Settlement Agreement is made and entered into by and between Plaintiffs, individually and on behalf of all Settlement Class Members, by and through their undersigned counsel of record, and PRGX.

NOW, THEREFORE, in consideration of the covenants, agreements, and releases set forth herein and for other good and valuable consideration the adequacy of which is hereby acknowledged, it is hereby agreed by and among Plaintiffs,

individually and on behalf of the Settlement Class, and PRGX that, subject to the approval of the Court, the Action be forever resolved, settled, compromised, and dismissed with prejudice on the following terms and conditions:

II. DEFINITIONS

16. The terms used in this Settlement Agreement, and listed in this section, shall have the following meanings:

- a. “Action” or “Complaint” means *Ebert, et al. v. PRGX Global, Inc*, No. 1:23-cv-04233 (N.D. Ga.).
- b. “Agreement” or “Settlement Agreement” or “Settlement” means this Settlement Agreement, Exhibits, and the settlement embodied herein.
- c. “Aggregate Cap” means the maximum amount to be paid by PRGX under this Settlement Agreement, which is no more than six hundred seventy-five thousand dollars (\$675,000.00).
- d. “PRGX” means PRGX Global, Inc.
- e. “PRGX’s Counsel” means Mullen Coughlin LLC.
- f. “Claim” means a claim for settlement benefits made under the terms of this Settlement Agreement.
- g. “Claimant” means a Settlement Class Member who makes a Claim for benefits under this Settlement Agreement.

- h. “Claims Administrator” means the third-party settlement administrator chosen by the Parties to provide Notice of the Settlement to the Settlement Class and administer the Settlement, subject to approval of the Court.
- i. “Claims Deadline” means the final time and date by which a Claim must be postmarked or submitted to the Settlement Website in order for a Class Member to be entitled to any of the settlement consideration contemplated by this Agreement. The Claims Deadline shall be ninety (90) days after the Notice Date.
- j. “Claim Form” means the form that the Settlement Class Member must complete and submit on or before the Claim Deadline in order to be eligible for the benefits described herein. The Claim Form shall be reformatted by the Settlement Administrator as needed. The Claim Form template is attached as Exhibit A to this Settlement Agreement.
- k. “Class Counsel” refers to William B. Federman of Federman & Sherwood.
- l. “Class Representatives” means Plaintiffs Jeffrey Ebert and Jennifer Ebert.
- m. “Court” means the United States District Court for the Northern District of Georgia, or such other Court sitting in its stead.

- n. “Days” means calendar days, except, when computing any period of time prescribed or allowed by this Settlement Agreement, does not include the day of the act, event, or default from which the designated period of time begins to run. Further, when computing any period of time prescribed or allowed by this Settlement Agreement, include the last day of the period, unless it is a Saturday, a Sunday, or a Federal legal holiday, in which event the period runs until the end of the next day that is not a Saturday, Sunday, or Federal legal holiday.
- o. “Effective Date of Settlement” or “Effective Date” means the date upon which the Settlement in the Action shall become effective and final, and occurs when the Final Judgment, as defined below, has been entered and all times to appeal therefrom have expired with (i) no appeal or other review proceeding having been commenced; or (ii) an appeal or other review proceeding having been commenced, and such appeal or other review having been concluded such that it is no longer subject to review by any court, whether by appeal, petitions for rehearing or re-argument, petitions for rehearing en banc, petitions for writ of certiorari, or otherwise, and such appeal or other review has been resolved in a manner that affirms the Final Judgment in all material respects.

- p. “Data Incident” means the Data Incident described in the Second Amended Class Action Complaint filed with Plaintiffs’ Motion for Preliminary Approval of Class Action Settlement, in which an unknown actor accessed PRGX’s systems between April 8, 2022, and April 9, 2022, and took or viewed certain files.
- q. “Extraordinary Losses” are documented unreimbursed costs or expenditures incurred by a Settlement Class Member due to identity theft and/or fraud. To receive reimbursement a Settlement Class Member must submit a Claim and supporting documentation showing:
- (i) the loss is an actual, documented, and unreimbursed monetary loss supported by third-party documentation;
 - (ii) the loss results from actual identity theft, fraud, or similar criminal victimization;
 - (iii) the loss was more likely than not caused by the Data Incident;
 - (iv) the loss is not already covered by one or more of the exemplar items listed in the Out-of-Pocket Losses, Time Spent, or Alternative Cash Payment categories;
 - and (v) the Settlement Class Member made reasonable efforts to avoid, mitigate, or seek reimbursement for, the loss, including but not limited to exhaustion of all available credit monitoring insurance and identity theft insurance. Examples of Extraordinary Losses may include, without limitation, monetary losses associated with falsified tax returns,

fraudulent transactions, false claims for government benefits, false claims for medical treatment, among others, incurred on or after April 8, 2022, through the date of the Settlement Class Member's Claim submission.

- r. "Fees, Costs, and Expenses" means the reasonable attorneys' fees, costs, and expenses incurred by counsel for Plaintiff and awarded by the Court, not to exceed the amount agreed to by the Parties.
- s. "Final Judgment" or "Final Approval" means a judgment entered by the Court, as discussed in Section XV, below following the Final Fairness Hearing.
- t. "Litigation" means all claims and causes of action asserted in the Action, or that could have been asserted, against PRGX and the Released Parties, including any and all appellate rights, as well as any other such actions by and on behalf of any other individuals or putative classes of individuals originating, or that may originate, in the jurisdictions of the United States against PRGX relating to the Data Incident. The Parties represent that they are unaware of any such actions pending other than the present Action.

- u. “Notice” means the postcard substantially in the form, included within Exhibit B, attached hereto, which will be mailed to Settlement Class Members via U.S.P.S. first class mail, subject to approval by the Court.
- v. “Notice Date” means the first date upon which the Notice is disseminated.
- w. “Opt-Out Date” means the date by which Settlement Class Members must submit their request to be excluded from the Settlement Class in order for that request to be effective.
- x. “Out-of-Pocket Losses” or “Out-of-Pocket Expenses” are documented unreimbursed costs or expenditures incurred by a Settlement Class Member as a result of the Data Incident from April 8, 2022, through the Claims Deadline, including costs associated with accessing or freezing/unfreezing credit reports; miscellaneous expenses such as bank fees, long distance phone charges, cell phone charges (only if charged by the minute), data charges (only if charged based on the amount of data used), postage, or gasoline for local travel relating to Out-of-Pocket Losses; and fees for credit reports, credit monitoring, or other identity theft insurance products purchased between April 8, 2022 and the date of the close of the Claims Period.

- y. “Parties” means Plaintiffs, on behalf of themselves and on behalf of the Settlement Class, and PRGX.
- z. “Person” means an individual, corporation, partnership, limited partnership, limited liability company or partnership, association, joint stock company, estate, legal representative, trust, unincorporated association, government or any political subdivision thereof, and any business or legal entity, and their respective spouses, heirs, predecessors, successors, representatives, agents and/or assignees.
- aa. “Plaintiffs” means Jeffrey Ebert, his minor children M.E., E.E., and S.E., and Jennifer Ebert.
- bb. “Preliminary Approval Order” means the proposed order preliminarily approving the Settlement and directing mailed notice to the Settlement Class of the pendency of the Action and of the Settlement, to be entered by the Court.
- cc. “Related Entities” means PRGX’s past or present parents, subsidiaries, divisions, and related or affiliated entities, and each of PRGX’s and their respective predecessors, successors, directors, officers, employees, principals, agents, attorneys, insurers, and reinsurers, and includes, without limitation, any Person related to any such entity who is, was, or could have been named as a defendant in the Litigation, other

than any Person who is found by a court of competent jurisdiction to be guilty under criminal law of initiating, causing, or aiding or abetting the criminal activity associated with the Data Security Incident or who pleads nolo contendere to any such charge.

dd. “Released Claims” means any and all past, present, and future claims, causes of action, counterclaims, lawsuits, rights, demands, charges, complaints, actions, obligations, or liabilities under any legal or equitable theory, whether known, unknown, suspected, or unsuspected or capable of being known or suspected, and whether, accrued, unaccrued, matured, or not matured, including, but not limited to, negligence, negligence *per se*, breach of implied contract, breach of fiduciary duty, unjust enrichment, intrusion into private affairs / invasion of privacy, and any other state or federal consumer protection statute, misrepresentation (whether fraudulent, negligent, or innocent), bailment, wantonness, failure to provide adequate notice pursuant to any breach notification statute, regulation, or common law duty, and any causes of action under 18 U.S.C. §§ 2701 *et seq.*, and all similar statutes in effect in any states in the United States as defined herein, and including, but not limited to, any and all claims for damages, injunctive relief, disgorgement, declaratory relief, equitable relief, attorneys’ fees,

costs and expenses, set-offs, losses, pre-judgment interest, credit monitoring services, the creation of a fund for future damages, statutory damages, punitive damages, special damages, exemplary damages, restitution, the appointment of a receiver, and any other form of relief that either has been asserted, or could have been asserted, by any Settlement Class Member against any of the Released Persons based on, relating to, concerning, or arising out of the Data Security Incident and alleged exposure and compromise of any Settlement Class Member's private information, personally identifiable information and/or protected health information, or any other allegations, facts, or circumstances described in the Litigation or the Complaint. Released Claims shall not include the right of any Settlement Class Member or any of the Released Persons to enforce the terms of the Settlement contained in this Settlement Agreement and shall not include the claims of Persons who have timely and validly requested exclusion from the Settlement Class pursuant to the opt-out procedures set forth in this Settlement Agreement.

ee. "Released Parties" means PRGX and all of its respective past, present, and future parent companies, partnerships, subsidiaries, affiliates, divisions, employees, servants, members, providers, partners,

principals, directors, shareholders, and owners, and all of its respective attorneys, heirs, executors, administrators, insurers, coinsurers, reinsurers, joint ventures, personal representatives, predecessors, successors, transferees, trustees, and assigns, and includes, without limitation, any Person related to any such entity who is, was, or could have been named as a Defendant in the Litigation.

ff. “Released Claims” means any and all past, present, and future claims, causes of action, counterclaims, lawsuits, rights, demands, charges, complaints, actions, obligations, or liabilities under any legal or equitable theory, whether known, unknown, suspected, or unsuspected or capable of being known or suspected, and whether, accrued, unaccrued, matured, or not matured, including, but not limited to, negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, intrusion into private affairs / invasion of privacy, and any other state or federal consumer protection statute, misrepresentation (whether fraudulent, negligent, or innocent), bailment, wantonness, failure to provide adequate notice pursuant to any breach notification statute, regulation, or common law duty, and any causes of action under 18 U.S.C. §§ 2701 et seq., and all similar statutes in effect in any states in the United States as defined herein, and

including, but not limited to, any and all claims for damages, injunctive relief, disgorgement, declaratory relief, equitable relief, attorneys' fees, costs and expenses, set-offs, losses, pre-judgment interest, credit monitoring services, the creation of a fund for future damages, statutory damages, punitive damages, special damages, exemplary damages, restitution, the appointment of a receiver, and any other form of relief that either has been asserted, or could have been asserted, by any Settlement Class Member against any of the Released Persons based on, relating to, concerning, or arising out of the Data Security Incident and alleged exposure and compromise of any Settlement Class Member's private information, personally identifiable information and/or protected health information, or any other allegations, facts, or circumstances described in the Litigation or the Complaint. Released Claims shall not include the right of any Settlement Class Member or any of the Released Persons to enforce the terms of the Settlement contained in this Settlement Agreement and shall not include the claims of Persons who have timely and validly requested exclusion from the Settlement Class pursuant to the opt-out procedures set forth in this Settlement Agreement.

gg. “Settlement Class” means all persons residing in the United States whose PHI and/or PII was potentially compromised in the Data Incident.

hh. “Unknown Claims” means any of the Released Claims that any Settlement Class Members, including any of the Class Representatives, does not know or suspect to exist in his/her favor at the time of the release of the Released Parties that, if known by him or her, might have affected his or her settlement with, and release of, the Released Parties, or might have affected his or her decision not to object to and/or to participate in this Settlement Agreement. With respect to any and all Released Claims, the Parties stipulate and agree that upon the Effective Date, the Class Representatives expressly shall have, and each of the other Settlement Class Members shall be deemed to have, and by operation of the Final Judgment shall have, waived the provisions, right, and benefits conferred by California Civil Code § 1542, and also any and all provisions, rights, and benefits conferred by the law of any state, province, or territory of the United States, which is similar, comparable, or equivalent to California Civil Code § 1542, which provides:

A GENERAL RELEASE DOES NOT EXTEND TO CLAIMS THAT THE CREDITOR OR RELEASING PARTY DOES

NOT KNOW OR SUSPECT TO EXIST IN HIS OR HER FAVOR AT THE TIME OF EXECUTING THE RELEASE AND THAT, IF KNOWN BY HIM OR HER, WOULD HAVE MATERIALLY AFFECTED HIS OR HER SETTLEMENT WITH THE DEBTOR OR RELEASED PARTY.

Settlement Class Members, including the Class Representatives, may hereafter discover facts in addition to, or different from, those that they now know or believe to be true with respect to the subject matter of the Released Claims, but the Class Representatives expressly shall have, and each other Settlement Class Member shall be deemed to have, and by operation of the Final Judgment shall have, upon the Effective Date, fully, finally, and forever settled and released any and all of the Released Claims. The Parties acknowledge, and Settlement Class Members shall be deemed by operation of the Final Judgment to have acknowledged, that the foregoing waiver is a material element of the Settlement Agreement of which this release is a part.

III. SETTLEMENT BENEFITS TO CLASS

17. **Out-of-Pocket Losses Reimbursement:** Settlement Class Members who suffered Out-of-Pocket Losses fairly traceable to the Data Incident, and timely submit a Claim supported by reasonable documentation of their Claim, will be eligible for a payment of up to six hundred dollars (\$600.00), but not more than the documented loss proven.

- a. Documentation supporting Out-of-Pocket Losses may include receipts or other documentation that documents the costs incurred. “Self-prepared” documents such as handwritten receipts are, by themselves, insufficient to receive reimbursement, but may be considered to add clarity to or support to other submitted documentation. Out-of-Pocket Losses that are compensated under this Settlement Agreement are those that are reasonable and customarily incurred when responding to this type of Data Incident and which occurred on or after April 8, 2022.
- b. **Time Spent:** A Settlement Class Member’s Claim for Out-of-Pocket Losses may also include a Claim for up to three (3) hours of attested-to lost time spent remedying identity theft or fraud, including misuse of personal information, credit monitoring or freezing credit reports, and/or other issues related to the Data Incident at thirty dollars (\$30.00) per hour (a maximum of ninety dollars (\$90.00) per Settlement Class Member) by providing a brief description of (i) the action taken in response to the Data Incident; (ii) the time associated with each action; and (iii) an attestation. No attestation or verification required or permitted by this Agreement shall require notarization.
18. **Extraordinary Losses Reimbursement:** Settlement Class Members who suffered Extraordinary Losses more likely than not caused by the Data Incident,

and who timely submit a Claim supported by reasonable documentation of their Claim, will be eligible for a payment of up to five thousand dollars (\$5,000.00), but not more than the documented loss proven. Documentation supporting Extraordinary Losses may include receipts or other documentation that documents the costs incurred. "Self-prepared" documents such as handwritten receipts are, by themselves, insufficient to receive reimbursement, but may be considered to add clarity to or support to other submitted documentation.

19. **Credit Monitoring Protections:** PRGX agrees to offer three (3) years of one (1) credit bureau credit monitoring and identity theft insurance through IDX. Settlement Class Members must affirmatively request credit monitoring by indicating such request on the Claim Form, and codes will be sent either to an email address provided by the Settlement Class Member or, if they do not have an email address, mailed to the address provided on the Claim Form.

20. **Alternative Cash Payment:** In lieu of receiving a reimbursement for Out-Of-Pocket Losses, Extraordinary Losses, Time Spent, and/or Credit Monitoring Protections, all Settlement Class Members may elect to submit a Claim for a one-time Alternative Cash Payment of up to seventy-five dollars (\$75.00). To receive the Alternative Cash Payment, Settlement Class Members must submit a valid Claim Form indicating the selection of an Alternative Cash Payment in lieu of all other benefits they may be eligible to receive under the Settlement Agreement. However,

the election to receive an alternative Cash payment does not preclude Class Representatives from receiving a Court approved Service Award Payment.

21. **Remedial Measures:** In response to the Data Breach, PRGX made business practice commitments intended to maintain or enhance its data security posture. These business practice commitments are set forth in a confidential declaration provided to Class Counsel. PRGX estimates that the cost of implementing these business practice commitments is \$300,000 - \$500,000. All costs and expenses incurred implementing these business practice commitments shall be paid by PRGX separate and apart from the Aggregate Cap.

IV. CONFIRMATORY DISCOVERY

22. PRGX has provided or will provide reasonable access to confidential confirmatory discovery regarding the number of Settlement Class Members and states of residents, the facts and circumstances of the Data Incident and PRGX's response thereto, and the changes and improvements that have been made or are being made to further protect Settlement Class Members' PII and PHI.

V. SECOND AMENDED CLASS ACTION COMPLAINT

23. After presenting to PRGX for its review and input as to form and content, Class Counsel shall submit a proposed Second Amended Class Action Complaint with their motion for Preliminary Approval, which will request that the Court permit the filing of the Second Amended Complaint in its Preliminary

Approval Order and pursuant to Fed. R. Civ. P. 15. In order to conform the operative pleading to the terms and scope of this Settlement, the Parties agree that the Second Amended Class Action Complaint will be filed for settlement purposes only and will assert class claims on behalf of a nationwide class regarding the Data Incident. The Second Amended Complaint shall be in the form attached hereto as **Exhibit D**. The Parties agree to cooperate and not oppose any actions necessary to effectuate the filing of a Second Amended Class Action Complaint.

VI. STIPULATED CLASS ACTION SETTLEMENT CERTIFICATION

24. Only for purposes of effectuating the Settlement, Class Representatives, Class Counsel, and PRGX agree and stipulate to certification of the Settlement Class as defined in this Agreement. Class Representatives, Class Counsel, and PRGX further agree and stipulate that, subject to Court approval, Class Counsel shall act as counsel for the Settlement Class.

25. Class Representatives, Class Counsel, and PRGX agree and stipulate that the Settlement should be approved by the Court, and that the Court should make a determination that the Settlement is fair, reasonable, and adequate, and made in good faith. Class Counsel and PRGX shall bear the expenses and responsibility for taking all necessary measures to obtain Court approval, including, without limitation, preparing and filing all papers with the Court necessary for obtaining such approval, and following the required procedures for a good faith determination.

26. Class Representative, Class Counsel, and PRGX agree and stipulate that the Parties shall timely submit the motions for Preliminary and Final Approval of the Parties' Settlement to the Court.

VII. RELEASE

27. On the Effective Date, the Parties and each and every Settlement Class Member shall be bound by this Settlement Agreement and shall have recourse only to the benefits, rights, and remedies provided hereunder. No other action, demand, suit, arbitration, or other claim may be pursued against PRGX or any Released Persons with respect to the Released Claims, as more specifically set forth in Paragraphs 27 through 33, below.

28. On the Effective Date and in consideration of the promises and covenants set forth in this Settlement Agreement, (i) Plaintiff and each Settlement Class Member, and each of their respective spouses and children with claims on behalf of the Settlement Class Member, executors, representatives, guardians, wards, heirs, estates, successors, predecessors, next friends, co-borrowers, co-obligors, co-debtors, legal representatives, attorneys, agents, and assigns, and all those who claim through them or who assert claims (or could assert claims) on their behalf (including the government in the capacity as *parens patriae* or on behalf of creditors or estates of the releasors), and each of them (collectively and individually, the "Releasing Persons"), and (ii) Class Counsel and each of their past and present law firms,

partners, or other employers, employees, agents, representatives, successors, or assigns will be deemed to have, and by operation of the Final Judgment shall have, fully, finally, completely, and forever released and discharged the Released Persons from the Released Claims. The release set forth in the preceding sentence (the “Release”) shall be included as part of any judgment, so that all Released Claims shall be barred by principles of res judicata, collateral estoppel, and claim and issue preclusion.

29. Without in any way limiting the scope of the Release, the Release covers, without limitation, any and all claims for attorneys’ fees, costs, and expenses incurred by Class Counsel or any other counsel representing Plaintiff or Settlement Class Members, or any of them, in connection with or related in any manner to the Litigation, the Settlement, the administration of such Settlement and/or the Released Claims, as well as any and all claims for the Service Award to Plaintiff.

30. Subject to Court approval, as of the Effective Date, all Settlement Class Members shall be bound by this Settlement Agreement and the Release and all of their claims shall be dismissed with prejudice and released, irrespective of whether they received actual notice of the Litigation or this Settlement.

31. As of the Effective Date, the Released Persons are deemed, by operation of the entry of the Final Order and Judgment, to have fully released and forever discharged Plaintiff, the Settlement Class Members, Class Counsel, or any

other counsel representing Plaintiff or Settlement Class Members, or any of them, of and from any claims arising out of the Litigation or the Settlement. Any other claims or defenses PRGX or other Released Persons may have against Plaintiff, the Settlement Class Members, Class Counsel, or any other counsel representing Plaintiff or Settlement Class Members, including, without limitation, any claims based upon or arising out of any employment, debtor-creditor, contractual, or other business relationship that are not based upon or do not arise out of the institution, prosecution, assertion, settlement, or resolution of the Litigation or the Released Claims are not released, are specifically preserved and shall not be affected by the preceding sentence.

32. As of the Effective Date, the Released Persons are deemed, by operation of entry of the Final Judgment, to have fully released and forever discharged each other of and from any claims they may have against each other arising from the claims asserted in the Litigation, including any claims arising out of the investigation, defense, or Settlement of the Litigation.

33. Nothing in the Release shall preclude any action to enforce the terms of this Settlement Agreement, including participation in any of the processes detailed herein.

VIII. ADMINISTRATION OF THE SETTLEMENT AND CLASS NOTICE

34. The Claims Administrator shall provide notice to the Settlement Class Members and administer the Settlement under the Parties' supervision and subject to the exclusive jurisdiction of this Court.

35. The Cost of providing notice to the Settlement Class Members shall be borne by PRGX, separate and apart from the Aggregate Cap.

36. Dissemination of the Notice shall be accomplished by the Claims Administrator and shall comply with the following:

- a. Class Member Information: No later than ten (10) days after entry of the Preliminary Approval Order, PRGX shall provide the Claims Administrator with the name and physical address of each Settlement Class Member (collectively, "Class Member Information") initially notified by mail of the Data Incident. PRGX agrees that it will provide the most current Class Member information in its possession for all Settlement Class Members from the updated mailing list in connection with the Data Incident responses related to the Data Incident.
- b. The Class Member Information and its contents shall be used by the Claims Administrator solely for the purpose of performing its obligations pursuant to this Agreement and shall not be used for any other purpose at any time. Except to administer the Settlement as

provided for in this Agreement, or to provide all data and information in its possession to the Parties upon request, the Claims Administrator shall not reproduce, copy, store, or distribute in any form, electronic or otherwise, the Class Member Information.

- c. Settlement Website: Prior to the dissemination of the Notice, the Parties agree to direct the Claims Administrator to create a website dedicated to providing information related to the Action and this Settlement, including the Long Form notice contained within Exhibit C. The website will include the information in the Notice, access to relevant publicly available court documents relating to the Action and provide Settlement Class Members with the ability to enroll in the Credit Monitoring Protections, make Claims for other Class benefits, and allow Settlement Class Members to submit documents to supplement or cure deficient Claims.
- d. Settlement Toll-Free Number: The Claims Administrator shall establish and maintain a toll-free telephone number with information relevant to this Settlement.
- e. Within twenty-one (21) days of receiving the Class Member Information, the Claims Administrator shall crosscheck the Class Member Information against the National Change of Address directory

to ensure the most recent and accurate addresses are used to disseminate the Notice. Upon receipt of any notice of address or forwarding address, the Claims Administrator shall re-mail any Notice so returned with a forwarding address.

- f. First Class Mail Notice: Within forty-five (45) days of receiving the Class Member Information, the Claims Administrator shall commence the dissemination of the Notice. Within fifteen (15) days thereafter, dissemination of the Notice shall be completed.
 - g. Notice shall be given by U.S.P.S. first class mail to all Settlement Class Members and postage will be prepaid by PRGX. U.S. Mail Notice shall consist of a postcard that (i) notifies Settlement Class Members of the Settlement and relevant terms (including opting-out of the Settlement and objecting to the Settlement); (ii) provides them with the URL to the Settlement Website and a telephone number they can call to obtain additional information about the Settlement; and (iii) instructs them on how to make a Claim.
 - h. All Settlement Class Members shall have ninety days (90) after the Notice Date to make Claims for Class benefits.
37. The administration of the Settlement is defined as the approval of the form of notice program and all related forms; initial mailing of the Notice; creation

and maintenance of Settlement Website; administration and coordination of the mailing and distribution of credit monitoring codes to be activated after final approval of Settlement;; day-to-day administration of the Settlement, including responding to Settlement Class Member inquiries; delivery to the Parties of any requests for opt-outs or objections; communication to the Parties about any issues that may arise; and the preparation of an Affidavit of Fairness of the Notice Program to be submitted to the Court with the Motion for Final Approval.

38. The notice program shall be designed to provide for maximum clarity and ease of Claim submission. Claims may be made by submitting a paper claim for by mail or by filling out an online Claim Form to be developed by the Claims Administrator.

39. The Claims Administrator shall inform Class Counsel and PRGX's Counsel regarding all material aspects of the claims process including Claims made, Claims accepted, Claims rejected, and all substantive communications with Settlement Class Members. Class Counsel may assist Settlement Class Members with the claims process and intercede with the Claims Administrator on their behalf.

40. Payments and credit monitoring codes for approved Claims shall be mailed or electronically submitted after the Effective Date and within forty (40) days of the Effective Date and/or forty (40) days of the date that the Claim is approved, whichever is latest.

41. Acceptance of payment is a condition precedent to any Settlement Class Member's right to receive Settlement benefits under Paragraphs 17 – 21. Payments shall be issued electronically, if possible and by check if electronic payment is not possible. All settlement checks shall be void one hundred and twenty (120) days after issuance and shall bear the language: "This check must be cashed within 120 days of its date, after which time it is void." If a check becomes void, the Settlement Class Member shall have an additional one hundred and twenty (120) days after the void date to request re-issuance. If no request for re-issuance is made within this period, the Settlement Class Member will have failed to meet a condition precedent to recovery of Settlement benefits under Paragraphs 17 – 21, the Settlement Class Member's right to receive monetary relief shall be extinguished, and PRGX shall have no obligation to make payments to the Settlement Class Member for expense reimbursement under Paragraphs 17 – 21 or any other type of monetary relief. The same provisions shall apply to any re-issued check. For any checks that are issued or re-issued for any reason more than two hundred and forty (240) days from the Effective Date, requests for re-issuance need not be honored after such checks become void, except for good cause as determined by the Claims Administrator in its professional judgment.

42. All Settlement Class Members who fail to timely submit a Claim for any benefits hereunder within the time frames set forth within, or such other period

as may be ordered by the Court, or otherwise allowed, shall be forever barred from receiving any payments or benefits pursuant to the Settlement set forth within, but will in all other respects be subject to, bound by, the provisions of the Settlement Agreement, the releases contained herein, and the Final Judgment.

43. No Person shall have any claims against the Claims Administrator, Class Representative, Class Counsel, PRGX, and/or PRGX's Counsel based on distribution of benefits to Settlement Class Members. Nothing contained herein shall be deemed a release of any claim against the Claims Administrator for its breach of fulfilling its duties due under its administration obligations.

IX. OPT-OUT PROCEDURES

44. Under the procedure set forth in the Notice, Settlement Class Members have the right and ability to exclude themselves from the Settlement Class as set forth in the proposed preliminary approval order. In order to validly be excluded from the Settlement, the Settlement Class Member must send a letter to the Claims Administrator no later than sixty (60) days after the Notice Date, stating that he or she wants to be excluded from the Settlement in the Action and include his or her name, address, and signature. If the opt-out is untimely or otherwise fails to comply with any of the provisions for a valid opt-out, it shall not be considered a valid opt-out.

45. All Persons who submit valid and timely notices of their intent to be excluded from the Settlement Class shall not receive any benefits of and/or be bound by the terms of this Settlement Agreement. All Persons falling within the definition of the Settlement Class who do not request to be excluded from the Settlement Class in the manner set forth in Paragraph 44, above, shall be bound by the terms of this Settlement Agreement and Final Judgment entered thereon. The Claims Administrator shall cause copies of requests for exclusion from Settlement Class Members to be provided to Class Counsel and PRGX's Counsel as they are received. No later than ten (10) days after the Opt-Out Date, the Claims Administrator shall provide Class Counsel and PRGX's Counsel a complete and final list of all known Settlement Class Members who have excluded themselves from the Settlement. Class Counsel shall provide this information to the Court before the Final Fairness Hearing.

X. OBJECTION PROCEDURES

46. The Notice will inform the Settlement Class Members that they may submit a written objection in this case, *Ebert, et al. v. PRGX Global, Inc.*, No. 1:23-cv-04233 (N.D. Ga.). To be valid, an objection must state: (i) the objector's full name, address, telephone number (if any), and email address (if any); (ii) information identifying the objector as a Settlement Class Member; (iii) a written statement of all grounds for the objection, accompanied by any legal support the

objector cares to submit; (iv) the identity of all lawyers (if any) representing the objector; (v) the identity of all of the objector's lawyers (if any) who will appear at the Final Fairness Hearing; (vi) a list of all persons who will be called to testify at the Final Fairness Hearing in support of the objection; (vii) a statement confirming whether the objector intends to personally appear and/or testify at the Final Fairness Hearing; and (viii) the objector's signature or the signature of the objector's duly authorized lawyer or other duly authorized representative.

47. In addition to the foregoing, objections should also provide the following information: (i) a list, by case name, court, and docket number, of all other cases in which the objector (directly or through a lawyer) has filed an objection to any proposed class action settlement within the last three (3) years; and (ii) a list, by case number, court, and docket number, of all other cases in which the objector has been a named Plaintiff any class action or served as a lead Plaintiff class representative.

48. The Notice will further inform Settlement Class Members that to be considered timely, any valid objection in the appropriate form must be filed with the Clerk for the United States District Court for the Northern District of Georgia no later than sixty (60) days after the Notice Date. The Notice will also inform Settlement Class Members that they must mail a copy of their objection to the

following three different places, postmarked no later than sixty (60) days after the

Notice Date:

Court	Class Counsel	PRGX'S Counsel
<p data-bbox="305 499 521 533">Clerk of Court</p> <p data-bbox="241 583 581 705">United States District Court for the Northern District of Georgia</p> <p data-bbox="207 753 613 1045">Richard B. Russell Federal Building & United States Courthouse 2211 United States Courthouse 75 Ted Turner Drive, SW Atlanta, GA 30303-3309</p>	<p data-bbox="678 499 1024 659">William B. Federman Federman & Sherwood 10205 N. Pennsylvania Ave.</p> <p data-bbox="651 669 1052 705">Oklahoma City, OK 73120</p>	<p data-bbox="1127 499 1393 659">Amanda Harvey Mullen Coughlin 1452 Hughes Rd., Suite 200</p> <p data-bbox="1094 669 1419 705">Grapevine, TX 76051</p>

49. The Parties agree that Plaintiffs will take the lead in drafting responses to any objections to the Settlement, including any appeals filed by the objectors. However, both Parties retain their rights to make any argument(s) in response to any objector.

50. Any Settlement Class Member who fails to comply with the requirements for objecting in this Section shall waive and forfeit any and all rights he or she may have to appear separately and/or to object to the Settlement Agreement and shall be bound by all the terms of the Settlement Agreement and by all proceedings, orders, and judgments in the Litigation. The exclusive means for any challenge to the Settlement Agreement shall be through the provisions of Section X.

Without limiting the foregoing, any challenge to the Settlement Agreement, the final order approving this Settlement Agreement, or the Final Judgment to be entered upon final approval, shall be pursuant to appeal and not through a collateral attack.

XI. DISPUTE RESOLUTION FOR CLAIMS

51. The Claims Administrator, in its sole discretion to be reasonably exercised, will determine whether: (i) the Claimant is a Settlement Class Member; (ii) the Claimant has provided all information needed to complete the Claim Form, including any documentation that may be necessary to reasonably support the claimed ordinary or extraordinary expenses, described above; and (iii) the information submitted could lead a reasonable person to conclude that more likely than not the Claimant has suffered the claimed losses as a result of the Data Incident (collectively, “Complete and Plausible”). The Claims Administrator may, at any time, request from the Claimant, in writing, additional information as the Claims Administrator may reasonably require in order to evaluate the Claim (“Claim Supplementation”), *e.g.*, documentation requested on the Claim Form, information regarding the claimed losses, available insurance and the status of any claims made for insurance benefits and claims previously made for identity theft and the resolution thereof.

52. The Claims Administrator’s initial review will be limited to a determination of whether the Claim is Complete and Plausible. For any such Claims

that the Claims Administrator determines to be implausible, the Claims Administrator will submit those Claims to the Parties. If the Parties agree that the Claimant's Claim is Complete and Plausible then the Claim shall be paid. If the Parties agree that the Claim is incomplete and/or implausible, it shall be denied. If the Parties do not agree, after meeting and conferring, then the Claim shall be referred to a mediator pursuant to agreement between the Parties (the "Claims Referee"), for resolution.

53. Upon receipt of an incomplete or unsigned Claim form or a Claim form that is not accompanied by sufficient documentation to determine whether the Claim is Complete and Plausible, the Claims Administrator shall request Claim Supplementation and give the Claimant thirty (30) days to cure the defect before rejecting the Claim. Requests for Claim Supplementation shall be made within thirty (30) days of receipt of such Claim form or thirty (30) days from the Effective Date, whichever comes later. In the event of unusual circumstances interfering with compliance during the 30-day period, the Claimant may request and, for good cause shown (illness, military service, out of the country, mail failures, lack of cooperation of third parties in possession of required information, etc.), shall be given a reasonable extension of the 30-day deadline in which to comply; however, in no event shall the deadline be extended to later than one year from the Effective Date.

If the defect is not cured, then the Claim will be deemed invalid and there shall be no obligation to pay the Claim.

54. Following receipt of additional information requested by the Claims Administrator, the Claims Administrator shall have thirty (30) days to accept, in whole or lesser amount, or reject each Claim. If, after review of the Claim and all documentation submitted by the Claimant, the Claims Administrator determines that such a Claim is Complete and Plausible, then the Claim shall be paid. If the Claim is not Complete and Plausible because the Claimant has not provided all information needed to complete the Claim form and evaluate the Claim, then the Settlement Administrator may reject the Claim. If the Claim is rejected in whole or in part, for other reasons, then the Claim shall be referred to the Parties. If the Parties agree that the Claimant's Claim is incomplete and/or implausible then no further action shall be taken. If the Parties agree that the Claimant's Claim is Complete and Plausible then the Claim shall be paid. If the Parties do not agree, after meeting and conferring, then the Claim shall be referred to the Claims Referee for resolution. Once a final determination regarding a Claim has been made, notice will be sent to the Claimant by the Claims Administrator regarding whether the Claim has been accepted, in whole or lesser amount, or rejected.

55. Settlement Class Members shall have thirty (30) days from receipt of the offer to accept or reject any offer of partial payment received from the Claims

Administrator. If a Settlement Class Member rejects an offer from the Claims Administrator, the Claims Administrator shall have fifteen (15) days to reconsider its initial adjustment amount and make a final determination. If the Claimant approves the final determination, then the approved amount shall be the amount to be paid. If the Claimant does not approve the final determination within thirty (30) days, then the dispute will be submitted to the Parties within an additional ten (10) days.

56. If any dispute cannot be resolved by the Parties and is submitted to the Claims Referee, the Claims Referee may approve the Claims Administrator's determination by making a ruling within fifteen (15) days. Alternatively, the Claims Referee may make any other final determination of the dispute or request further supplementation of a Claim within thirty (30) days. The Claims Referee's determination shall be based on whether the Claims Referee is persuaded that the claimed amounts are reasonably supported in fact and were more likely than not caused by the Data Incident. The Claims Referee shall have the power to approve a Claim in full or in part. The Claims Referee's decision will be final and non-appealable. Any Claimant referred to the Claims Referee shall reasonably cooperate with the Claims Referee, including by either providing supplemental information as requested or, alternatively, signing an authorization allowing the Claims Referee to verify the Claim through third party sources, and failure to cooperate shall be

grounds for denial of the Claim in full. The Claims Referee shall make a final decision within thirty (30) days of receipt of all supplemental information requested.

XII. NOTICE AND ADMINISTRATION EXPENSES

57. All costs of notice and administration, including without limitation, the fees and expenses of the Claims Administrator and Claims Referee, shall be paid separately and apart from the Aggregate Cap by PRGX directly to the Claims Administrator, Claims Referee, or other party.

XIII. ATTORNEYS' FEES, COSTS, EXPENSES AND SERVICE AWARDS

58. PRGX will pay the attorneys' fees, costs, and expenses incurred by Class Counsel in the Action, as approved by the Court, three hundred thousand dollars (\$300,000.00), separate and apart from the Aggregate Cap.

59. PRGX will pay a Service Award of one thousand seven hundred fifty dollars (\$1,750.00) to each of the Class Representatives—Jeffrey Ebert and Jennifer Ebert.

60. The Parties did not discuss or agree upon payment of attorneys' fees, costs, expenses and Service Awards until after they agreed on all material terms of relief to the Settlement Class.

61. Any attorneys' fees, costs, expenses and Service Awards awarded by the Court shall be paid within twenty-one (21) days after the Effective Date of Settlement.

62. PRGX shall pay any attorneys' fees, costs, expenses and Service Awards as set forth above, to accounts established by Class Counsel. Such account(s) shall be disclosed to PRGX within seven (7) days after the Court has granted Final Approval.

63. The amount(s) of each award of attorneys' fees, costs, expenses, and Service Awards are intended to be considered by the Court separately from the Court's consideration of the fairness, reasonableness, and adequacy of the Settlement. Class Counsel will file a fee petition within two (2) weeks of the Final Fairness Hearing. PRGX will not oppose Class Counsel's request for reasonable attorneys' fees, costs, expenses, and Service Awards. No order of the Court, or modification or reversal or appeal of any order of the Court, concerning the amount(s) of any attorneys' fees, costs, expenses, and Service Awards ordered by the Court to the Class Counsel shall affect whether the Settlement becomes effective and final or constitute grounds for cancellation or termination of this Settlement Agreement, except that the payment of the attorneys' fees, costs, expenses, and Service Awards as agreed to in Paragraphs 58 and 59, will not be paid until any appeal or other review proceeding regarding the attorneys' fees, costs, and expenses has been resolved.

XIV. PRELIMINARY APPROVAL OF SETTLEMENT

64. After the execution of the Settlement Agreement, Class Counsel and PRGX's Counsel shall jointly submit this Settlement Agreement to the Court and file a Motion for Preliminary Approval of the Settlement with the Court requesting entry of the Preliminary Approval Order attached to Plaintiffs' Motion for Preliminary Approval, or an order substantially similar to such form, requesting, *inter alia*:

- a. Certification of the Settlement Class for settlement purposes only;
- b. Preliminary approval of the Settlement Agreement as set forth herein;
- c. Appointment of Class Counsel as counsel for the Settlement Class;
- d. Appointment of Class Representatives as representatives for the Settlement Class;
- e. Approval of a form of notice, which includes a notice to be individually mailed to the Settlement Class Members, as well as a detailed long form notice that will be posted on the Settlement Website;
- f. Appointment of a Claims Administrator as jointly agreed by the Parties.

XV. FINAL JUDGMENT

65. If the Preliminary Approval Order is entered by the Court, Class Counsel will move the Court, within the time frames contemplated by the Preliminary Approval Order, for entry of a Final Judgment.

66. Upon entry of a Final Judgment, Plaintiffs shall move to dismiss the Action with prejudice.

XVI. TERMINATION

67. If the Effective Date of Settlement does not occur, or if the Settlement is terminated or fails to become effective for any reason, then (a) the Parties shall be restored to their respective positions in the Action and shall jointly request that all scheduled litigation deadlines be reasonably extended by the Court so as to avoid prejudice to any Party or Party's counsel; and (b) the terms and provisions of the Settlement Agreement and statements made in connection with seeking approval of the Agreement shall have no further force and effect with respect to Parties and shall not be used in the Action or in any other proceeding for any purpose, and any judgment or order entered by the Court in accordance with the terms of the Settlement Agreement shall be treated as vacated, nunc pro tunc.

XVII. NO ADMISSION OF WRONGDOING OR LACK OF MERIT

68. The terms of this Settlement (whether the Settlement becomes final or not), the negotiations leading up to this Settlement, the fact of the Settlement, and the proceedings taken pursuant to the Settlement, shall not: (a) be construed as an admission of liability or an admission of any claim or defense on the part or any Party, in any respect; (b) form the basis for any claim of estoppel by any third-party against any of the Released Parties; or (c) be admissible in any action, suit,

proceeding, or investigation as evidence, or as an admission of any wrongdoing or liability whatsoever by any Party, or as evidence of the truth of any of the claims or allegations contained in the Complaint.

XVIII. MISCELLANEOUS PROVISIONS

69. All of the exhibits attached hereto are hereby incorporated by reference as though fully set forth herein.

70. The Parties to the Settlement intend and agree that the Settlement is a final and complete resolution of all disputes related to the Litigation by the Class Representative and the Settlement Class Members who have not timely excluded themselves from the Settlement.

71. The Parties agree that the benefits provided herein and the other terms of the Settlement were negotiated at arm's length in good faith by the Parties to the Settlement with the assistance of an experienced and independent mediator and reflect a settlement that was reached voluntarily after consultation with experienced legal counsel.

72. This Settlement may not be modified or amended, nor may any of its provisions be waived, except by a writing signed by all Parties or their successors-in-interest.

73. The headings herein are used for the purpose of convenience only and are not meant to have legal effect.

74. The Parties hereby irrevocably submit to the continuing and exclusive jurisdiction of the Court for any suit, action, proceeding, or disputing arising out of or relating to this Settlement as embodied in the Settlement or its applicability, and agree that they will not oppose the designation of such suit, action, proceeding, or dispute as a related case to the Action.

75. The Settlement may be executed in one or more counterparts. All executed counterparts and each of them shall be deemed to be one and the same instrument, provided that counsel for the Parties to the Settlement shall exchange among themselves original signed counterparts. Electronically transmitted signatures are valid signatures as of the date thereof.

76. The construction, interpretation, operation, effect, and validity of the Settlement, and all documents necessary to effectuate it, shall be governed by the laws of the State of Georgia. The Parties understand and agree that any disputes arising out of the Settlement shall be governed and construed by and in accordance with the laws of the State of Georgia.

77. The Settlement shall not be construed more strictly against one Party to the Settlement than another merely by virtue of the fact that it, or any part of it, may have been prepared by counsel for one of the Parties, it being recognized that the Settlement is the result of arm's-length negotiation between the Parties to the

Settlement, and all Parties to the Settlement have contributed substantially and materially to the preparation of the Settlement.

78. Any and all counsel and Parties to the Settlement who execute the Settlement and any of the exhibits hereto, or any related Settlement documents, represent that they have reviewed and understand those documents and have the full authority to execute the Settlement, and that they have the authority to take appropriate action required or permitted to be taken pursuant to the Settlement to effectuate its terms.

79. Class Counsel and PRGX's Counsel agree to recommend approval of the Settlement by the Court and to undertake their best efforts and cooperate fully with one another in seeking Court approval of the Preliminary Approval Order and the Settlement and to promptly agree upon and execute all such other documentation as may be reasonably required to obtain final approval by the Court of the Settlement and the entry of the Final Judgment.

IN WITNESS WHEREOF, the Parties have, through their respective counsel, executed this Settlement Agreement as of the date first written above.

Approved as to form and content by Plaintiffs and counsel for Plaintiffs and the Settlement Class:

DocuSigned by:
Jeffrey Ebert
/s/ _____
7E4493C32D8C4D4...
Jeffrey Ebert

DocuSigned by:
Jennifer Ebert
/s/ _____
7329EDBB6E6E7A2...
Jennifer Ebert

/s/ *William B. Federman*

William B. Federman
Lead Counsel
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
P: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com

Approved as to form and content by Defendant and counsel for PRGX Global, Inc.:

DocuSigned by:
Rodrigo Hoefel
/s/ _____
DC3555000856402...
PRGX Global, Inc.

/s/ *Amanda N. Harvey*

Amanda N. Harvey
Mullen Coughlin LLC
1452 Hughes Rd, Suite 200
Grapevine, TX 76051
T: (267) 930-1697
E: aharvey@mullen.law

Exhibit A

Your claim must be
submitted online or
postmarked by:
[DEADLINE]

Ebert, et al. v. PRGX Global, Inc.
Case No. 1:23-cv-04233-TWT
U.S.D.C. Northern District of Georgia – Atlanta Division.

**PRGX-
CLAIM**

CLAIM FORM

GENERAL INSTRUCTIONS

Complete this Claim Form if you are a Settlement Class Member and you wish to receive Settlement benefits.

You are a member of the Settlement Class and eligible to submit a Claim Form if:

You are an individual who resides in the United States whose private information was impacted by the cybersecurity incident that affected PRGX or around April 2022 (“Data Incident”).

Excluded from the Settlement Class are (i) PRGX, its officers and directors; (ii) all Settlement Class Members who timely and validly request exclusion from the Settlement Class; (iii) any judges assigned to this case and their staff and family; and (iv) any other person found by a court of competent jurisdiction to be guilty under criminal law of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Incident or who pleads *nolo contendere* to any such charge.

Settlement Class Members may submit a claim form for: (i) 3 years of credit monitoring; (ii) reimbursement of Out-of-Pocket Losses up to a total of \$600 per claimant; (iii) reimbursement of Lost Time at a rate of \$30.00 per hour for up to 3 hours (a total of \$90, subject to the \$600 cap on Out-of-Pocket Loss claims); and (iv) reimbursement of Extraordinary Losses up to a total of \$5,000 per claimant. Settlement Class Members may also elect to receive an Alternative Cash Payment up to \$75 per person in lieu of making a claim for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring services.

Credit Monitoring Services. Settlement Class Members may submit a claim for 3 years of credit monitoring and identity theft protection services by selecting this benefit on this Claim Form.

Out-of-Pocket Losses. Settlement Class Members may submit a claim for reimbursement of Out-of-Pocket Losses up to \$600.00 per claimant, with supporting documentation. The loss must have occurred on or after April 8, 2022. Out-of-Pocket Losses include, but are not limited to, costs associated with accessing or freezing/unfreezing credit reports; miscellaneous expenses such as bank fees, long distance phone charges, cell phone charges (only if charged by the minute), data charges (only if charged based on the amount of data used), postage, or gasoline for local travel relating to Out-of-Pocket Losses; and fees for credit reports, credit monitoring, or other identity theft insurance products purchased between April 8, 2022 and the date of the close of the Claims Period.

Time Spent. Settlement Class Members may submit a claim for a reimbursement for time spent addressing the Data Incident at a rate of \$30.00 per hour for up to 3 hours (a total of \$90) with a brief description of the activities engaged in, the time spent on each activity, and an attestation on the Claim Form that the activities performed were related to the Data Incident. Claims for Lost Time are subject to the \$600.00 cap for Out-of-Pocket Losses.

Extraordinary Losses. Settlement Class Members may submit a claim for reimbursement of Extraordinary Losses up to \$5,000.00 per Settlement Class Member. Extraordinary Losses must meet the following conditions: (i) The loss is an actual, documented, and unreimbursed monetary loss supported by third-party documentation; (ii) The loss results from actual identity theft, fraud, or similar criminal victimization; (iii) The loss was more likely than not caused by the Data Incident; (iv) The loss is not already covered by one or more of the exemplar items listed in the Out-of-Pocket Losses, Time Spent, or Alternative Cash Payment categories; and/or (v) The Settlement Class Member made reasonable efforts to avoid, mitigate, or seek reimbursement for, the loss, including but not limited to exhaustion of all available credit monitoring insurance and identity theft insurance.

Alternative Cash Payment. Settlement Class Members may also elect to receive an Alternative Cash Payment up to \$75 per person in lieu of making a claim for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring services.

In the unlikely event that the total Settlement Benefits claimed exceed \$675,000, the cost of credit monitoring will be paid as a first priority; other costs and expenses will be pro-rated as needed to stay within the maximum \$675,000 cap.

Your claim must be submitted online or postmarked by: **[DEADLINE]**

Ebert, et al. v. PRGX Global, Inc.
Case No. 1:23-cv-04233-TWT
U.S.D.C. Northern District of Georgia – Atlanta Division.

PRGX-CLAIM

CLAIM FORM

TOTAL AMOUNT CLAIMED: _____

IV. CREDIT MONITORING SERVICES

Check this box if you wish to enroll in credit monitoring services for 3 years, which includes credit monitoring through **[Add]** and \$1,000,000 in identity theft insurance.

V. ALTERNATIVE CASH PAYMENT

Check this box if you wish to receive a one-time \$75 payment in lieu of making a claim for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring services.

VI. PAYMENT SELECTION

Please select **one** of the following payment options, which will be used should you be eligible to receive a Settlement payment:

PayPal - Enter your PayPal email address: _____

Venmo - Enter the mobile number associated with your Venmo account: _____ - _____ - _____

Zelle - Enter the mobile number or email address associated with your Zelle account:

Mobile Number: _____ - _____ - _____ or Email Address: _____

Virtual Prepaid Card - Enter your email address: _____

Physical Check - Payment will be mailed to the address provided in Section I above.

VII. ATTESTATION & SIGNATURE

I swear and affirm that the information provided in this Claim Form, and any supporting documentation provided is true and correct to the best of my knowledge. I understand that my claim is subject to verification and that I may be asked to provide supplemental information by the Settlement Administrator before my claim is considered complete and valid.

Signature

Printed Name

Date

Exhibit B

**NOTICE OF CLASS
ACTION SETTLEMENT**

**If you received this
Notice, you have been
identified as someone
eligible to submit a claim
under a class action
settlement regarding a
Data Incident affecting
PRGX Global, Inc.
«Settlement Website»**

PRGX Data Incident Settlement
c/o Settlement Administrator
1650 Arch Street, Suite 2210
Philadelphia, PA 19103

«ScanString»

Postal Service: Please do not mark barcode

Notice ID: «Notice ID»

Confirmation Code: «Confirmation Code»

«FirstName» «LastName»

«Address1»

«Address2»

«City», «StateCd» «Zip»

«CountryCd»

What is this Litigation about? The Litigation *Ebert, et al. v. PRGX Global, Inc.*, Case No. 1:23-cv-04233-TWT, alleges that on or around April 8, 2022, PRGX Global, Inc. ("PRGX") suffered a data security incident where certain private information belonging to PRGX's current and former employees was subject to unauthorized access (the "Data Incident"). You are a Settlement Class Member if you are a Person in the United States to whom PRGX mailed a notification that your information may have been impacted in the Data Incident.

What are the Settlement Benefits and terms? Settlement Class Members who file a Valid Claim may receive: (i) 3 years of Credit Monitoring; (ii) reimbursement for Out-of-Pocket Losses up to a total of \$600 per claimant; (iii) reimbursement for Time Spent at a rate of \$30.00 per hour for up to 3 hours (a total of \$90, subject to the \$600 cap on Out-of-Pocket Loss claims); and/or (iv) reimbursement for Extraordinary Losses up to a total of \$5,000 per claimant. Settlement Class Members may elect to receive an Alternative Cash Payment of \$75 in lieu of reimbursement for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring Services. More information is available on the Settlement Website.

What are your rights and options?

Submit a Claim Form. To qualify for Settlement Benefits, you must timely mail a Claim Form or timely complete and submit a Claim Form online at www.xxxxxxxxxxxxxxxxxx.com. Your Claim Form must be postmarked or submitted online no later than the Claims Deadline of **<<Claims Deadline>>**.

Opt-Out. You may exclude yourself from the settlement and retain your ability to sue Defendant on your own by mailing a Request for Exclusion to the Settlement Administrator that is postmarked no later than **<< Opt-Out Date>>**. If you do not exclude yourself, you will be bound by the settlement and give up your right to sue regarding the Released Claims.

Object. If you do not exclude yourself, you have the right to object to the settlement. Written objections must be signed, postmarked no later than

<<Objection Date>>. You may also appear at the Final Fairness Hearing. Further instructions can be found on the Long Notice and in the Settlement Agreement located on the Settlement Website www.xxxxxxxxxxxxxxxxxx.com.

Do Nothing. If you do nothing, you will not receive a Settlement Payment and will lose the right to sue regarding the Released Claims. You will be bound by the Court's decision because this is a conditionally certified class action.

Attend the Final Fairness Hearing. The Court will hold a Final Fairness Hearing at **<<time>>** on **<<Date>>**, to determine if the settlement is fair, reasonable, and adequate. All Persons who timely object to the settlement may appear at the Final Fairness Hearing.

Who are the attorneys for the Plaintiffs and the proposed Settlement Class?

The Court appointed William B. Federman of Federman & Sherwood to represent the Settlement Class. If you want to be represented by your own lawyer, you may hire one at your own expense.

Do I have any obligation to pay attorneys' fees or expenses?

No. Settlement Class Counsel will file a motion for an award of attorneys' fees and litigation costs and expenses up to \$300,000. The Fee Award and Costs will be paid separate and apart from the from the Aggregate Cap, if approved by the Court. The motion will be posted on the Settlement Website after it is filed with the Court.

What is the amount of the Representative Plaintiffs' Service Awards?

The Plaintiffs, or "Class Representatives" will seek Service Awards up to \$1,750 each for their time, effort and service to the Settlement Class in this matter.

Where may I locate a copy of the Settlement Agreement, learn more about the case or learn more about submitting a Settlement Claim?
www.xxxxxxxxxxxxxxxxxx.com

This notice is a summary of the proposed settlement.

Exhibit C

NOTICE OF PROPOSED CLASS ACTION SETTLEMENT

U.S.D.C. Northern District of Georgia – Atlanta Division
Ebert, et al. v. PRGX Global, Inc.
Case No. 1:23-cv-04233-TWT

**IF YOUR PRIVATE INFORMATION WAS IMPACTED BY A
CYBERSECURITY INCIDENT THAT PRGX EXPERIENCED
IN APRIL 2022, A PROPOSED CLASS ACTION
SETTLEMENT MAY AFFECT YOUR RIGHTS**

*A federal court authorized this Notice. You are not being sued.
This is not a solicitation from a lawyer.*

- A settlement has been reached with PRGX Global, Inc., (“Defendant” or “PRGX”) in a class action lawsuit about a cybersecurity incident that occurred in or around April 2022 (“Settlement”).
- The lawsuit is captioned *Jeffrey Ebert, on behalf of himself and his minor children M.E., E.E., and S.E., and Jennifer Ebert, on behalf of herself and collectively on behalf of all others similarly situated v. PRGX Global, Inc.*, Case No. 1:23-cv-04233-TWT, U.S.D.C. Northern District of Georgia – Atlanta Division. PRGX denies the allegations and all liability or wrongdoing with respect to any and all facts and claims alleged in the lawsuit but has agreed to a settlement to avoid the costs and risks associated with continuing this case.
- You are included in this Settlement if you are a Settlement Class Member. A Settlement Class Member is an individual who resides in the United States whose private information was impacted by the cybersecurity incident that affected PRGX in or around April 2022.
- Your rights are affected whether you act or don’t act. Please read this Notice carefully.

SUMMARY OF YOUR LEGAL RIGHTS AND OPTIONS IN THIS SETTLEMENT		DEADLINE
SUBMIT A CLAIM	<p>The only way to receive cash and other benefits from this Settlement is by submitting a valid and timely Claim Form.</p> <p>You can submit your Claim Form online at [REDACTED] or download the Claim Form from the Settlement Website and mail it to the Settlement Administrator. You may also call or email the Settlement Administrator to receive a paper copy of the Claim Form.</p>	[REDACTED], 2024
OPT OUT OF THE SETTLEMENT	You can choose to opt out of the Settlement and receive no payment. This option allows you to sue, continue to sue, or be part of another lawsuit against the Defendant related to the legal claims resolved by this Settlement. You can elect to retain your own legal counsel at your own expense.	[REDACTED], 2024
OBJECT TO THE SETTLEMENT AND/OR ATTEND A HEARING	If you do not opt out of the Settlement, you may object to it by writing to the Court about why you don't like the Settlement. You may also ask the Court for permission to speak about your objection at the Final Approval Hearing. If you object, you may also file a claim for benefits.	[REDACTED], 2024
DO NOTHING	Unless you opt out of the settlement, you are part of the Settlement. If you do nothing, you will not get a payment from this Settlement and you will give up the right to sue, continue to sue, or be part of another lawsuit against the Defendant related to the legal claims resolved by this Settlement.	No Deadline

- These rights and options—**and the deadlines to exercise them**—are explained in this Notice.
- The Court in charge of this case still has to decide whether to approve the Settlement.

WHAT THIS NOTICE CONTAINS

BASIC INFORMATION**Error! Bookmark not defined.**

WHO IS IN THE SETTLEMENT 4

THE SETTLEMENT BENEFITS..... 4

HOW TO GET A PAYMENT—MAKING A CLAIM..... 5

THE LAWYERS REPRESENTING YOU 6

OPTING OUT OF THE SETTLEMENT..... 7

COMMENTING ON OR OBJECTING TO THE SETTLEMENT 7

THE COURT’S FINAL APPROVAL HEARING 8

IF I DO NOTHING 9

GETTING MORE INFORMATION 9

BASIC INFORMATION

1. Why was this Notice issued?

A federal court (the “Court”) authorized this Notice because you have a right to know about the proposed Settlement of this class action lawsuit and about all your options before the Court decides whether to grant final approval of the Settlement. This Notice explains the lawsuit, your legal rights, what benefits are available, and who can receive them.

The lawsuit is captioned *Jeffrey Ebert, on behalf of himself and his minor children M.E., E.E., and S.E., and Jennifer Ebert, on behalf of herself and collectively on behalf of all others similarly situated v. PRGX Global, Inc.*, Case No. 1:23-cv-04233-TWT, U.S.D.C. Northern District of Georgia – Atlanta Division. The individuals that filed this lawsuit are called the “Plaintiffs” and the company they sued, PRGX, is called the “Defendant.”

2. What is this lawsuit about?

This lawsuit alleges that private information was impacted by the cybersecurity incident that affected PRGX in or around April 2022 (“Data Incident”).

3. What is a class action?

In a class action, one or more individuals sue on behalf of other people with similar claims. These individuals are known as “Class Representatives” or “Plaintiffs.” Together, the people included in the class action are called a “class” or “class members.” One court resolves the lawsuit for all settlement class members, except for those who opt out from a settlement. In this Settlement, the Class Representatives are Jeffrey Ebert and Jennifer Ebert.

4. Why is there a Settlement?

The Court did not decide in favor of the Plaintiffs or the Defendant. The Defendant denies all claims and contends that it has not violated any laws. The Plaintiffs and the Defendant agreed to a Settlement to avoid the costs and risks of a trial, and through the Settlement, Settlement Class Members are eligible to receive payments. The Plaintiffs and their attorneys think the Settlement is best for all Settlement Class Members.

WHO IS IN THE SETTLEMENT?

5. Who is included in the Settlement?

The Settlement Class consists of all individuals, or their respective successors or assigns, who reside in the United States and to whom Defendant sent a notice concerning the Data Incident.

6. Are there exceptions to being included?

Yes. Excluded from the Settlement Class are (i) PRGX, its officers and directors; (ii) all Settlement Class Members who timely and validly request exclusion from the Settlement Class; (iii) any judges assigned to this case and their staff and family; and (iv) any other person found by a court of competent jurisdiction to be guilty under criminal law of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Incident or who pleads *nolo contendere* to any such charge.

If you are not sure whether you are included in the Settlement Class, you can ask for free help by emailing or writing to Settlement Administrator at:

[email address]

PRGX Data Incident, c/o Settlement Administrator, 1650 Arch Street, Suite 2210, Philadelphia, PA 19103

You may also view the Settlement Agreement and Release (“Settlement Agreement”) at [Website URL].

THE SETTLEMENT BENEFITS

7. What does the Settlement provide?

Under the Settlement, PRGX will pay all valid and timely claims for Credit Monitoring, Ordinary Losses, Lost Time, Extraordinary Losses, and Alternative Cash Payments up to an aggregate cap of \$675,000.

8. How much will my payment be?

Payments will vary - Settlement Class Members may submit a claim form for: (i) 3 years of credit monitoring; (ii) reimbursement of Out-of-Pocket Losses up to a total of \$600 per claimant; (iii) reimbursement of Lost Time at a rate of \$30.00 per hour for up to 3 hours (a total of \$90, subject to

the \$600 cap on Out-of-Pocket Loss claims); and/or (iv) reimbursement of Extraordinary Losses up to a total of \$5,000 per claimant. Settlement Class Members may also elect to receive an Alternative Cash Payment up to \$75 per person in lieu of making a claim for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring services.

Credit Monitoring Services. Settlement Class Members may submit a claim for 3 years of credit monitoring and identity theft protection services by selecting this benefit on the Claim Form.

Out-of-Pocket Losses. Settlement Class Members may submit a claim for reimbursement of Out-of-Pocket Losses up to \$600.00 per claimant, with supporting documentation. The loss must have occurred on or after April 8, 2022. Out-of-Pocket Losses include, but are not limited to, costs associated with accessing or freezing/unfreezing credit reports; miscellaneous expenses such as bank fees, long distance phone charges, cell phone charges (only if charged by the minute), data charges (only if charged based on the amount of data used), postage, or gasoline for local travel relating to Out-of-Pocket Losses; and/or fees for credit reports, credit monitoring, or other identity theft insurance products purchased between April 8, 2022 and the date of the close of the Claims Period.

Time Spent. Settlement Class Members may submit a claim for reimbursement for time spent addressing the Data Incident at a rate of \$30.00 per hour for up to 3 hours (a total of \$90) with a brief description of the activities engaged in, the time spent on each activity, and an attestation on the Claim Form that the activities performed were related to the Data Incident. Claims for Lost Time are subject to the \$600.00 cap for Out-of-Pocket Losses.

Extraordinary Losses. Settlement Class Members may submit a claim for reimbursement of Extraordinary Losses up to \$5,000.00 per Settlement Class Member. Extraordinary Losses must meet the following conditions: (i) The loss is an actual, documented, and unreimbursed monetary loss supported by third-party documentation; (ii) The loss results from actual identity theft, fraud, or similar criminal victimization; (iii) The loss was more likely than not caused by the Data Incident; (iv) The loss is not already covered by one or more of the exemplar items listed in the Out-of-Pocket Losses, Time Spent, or Alternative Cash Payment categories; and (v) The Settlement Class Member made reasonable efforts to avoid, mitigate, or seek reimbursement for, the loss, including but not limited to exhaustion of all available credit monitoring insurance and identity theft insurance.

Alternative Cash Payment. Settlement Class Members may also elect to receive an Alternative Cash Payment up to \$75 per person in lieu of making a claim for Out-of-Pocket Losses, Time Spent, Extraordinary Losses, and Credit Monitoring services.

In the unlikely event that the total Settlement Benefits claimed exceed \$675,000, the cost of credit monitoring will be paid as a first priority; other costs and expenses will be pro-rated as needed to stay within the maximum \$675,000 cap.

9. What claims am I releasing if I stay in the Settlement Class?

Unless you opt out of the Settlement, you cannot sue, continue to sue, or be part of any other lawsuit against the Defendant about any of the legal claims this Settlement resolves. The “Releases” section in the Settlement Agreement describes the legal claims that you give up if you remain in the Settlement Class. The Settlement Agreement can be found at [\[Website URL\]](#).

HOW TO GET A PAYMENT - MAKING A CLAIM

10. How do I submit a claim and get a cash payment?

You may file a claim if you are an individual who resides in the United States who received notice of the Data Incident from PRGX.

Claim Forms may be submitted online at [Website URL] or printed from the website and mailed to the Settlement Administrator at: PRGX Data Incident, c/o Settlement Administrator, Attn: Claim Forms, 1650 Arch Street, Suite 2210, Philadelphia, PA 19103.

You may also contact the Settlement Administrator to request a Claim Form by telephone 1-XXX-XXX-XXXX, by email [Email Address], or by U.S. mail at the address above.

11. What is the deadline for submitting a claim?

If you submit a claim by U.S. mail, the completed and signed Claim Form must be postmarked by [Deadline Date]. If submitting a Claim Form online, you must do so by [Deadline Date].

12. When will I get my payment?

The Court is scheduled to hold a final approval hearing on _____, 2024 to decide whether to approve the Settlement, how much attorneys' fees and costs to award to Settlement Class Counsel for representing the Settlement Class, and whether to award Service Awards to the Class Representatives who brought this Action on behalf of the Settlement Class.

If the Court approves the Settlement, there may be appeals. It is always uncertain whether appeals will be filed and, if so, how long it will take to resolve them. Settlement payments will be distributed as soon as possible, if and when the Court grants final approval to the Settlement and after any appeals are resolved.

THE LAWYERS REPRESENTING YOU

13. Do I have a lawyer in the case?

Yes, the Court appointed William B. Federman of Federman & Sherwood to represent you and other members of the Settlement Class ("Settlement Class Counsel"). You will not be charged directly for these lawyers; instead, they will receive compensation from PRGX (subject to Court approval). If you want to be represented by your own lawyer, you may hire one at your own expense.

14. Should I get my own lawyer?

It is not necessary for you to hire your own lawyer because Settlement Class Counsel works for you. If you want to be represented by your own lawyer, you may hire one at your own expense.

15. How will the lawyers be paid?

Settlement Class Counsel will file a motion for an award of attorneys' fees and litigation costs and expenses to be paid by PRGX. PRGX has agreed not to oppose Settlement Class Counsel's request for an award of attorneys' fees and litigation costs and expenses not to exceed Three Hundred Thousand

Dollars and Zero Cents (\$300,000.00). If Settlement Class Counsel seeks more than \$300,000.00 in attorneys' fees and expenses, PRGX has reserved all rights to object and oppose such requests. Any attorneys' fees and litigation costs and expenses awarded will be paid separate and apart from the aggregate cap.

Settlement Class Counsel will also seek a service award payment for the Class Representatives in recognition for their contributions to this Action. PRGX has agreed not to oppose Settlement Class Counsel's request for service awards not to exceed One Thousand Dollars and Seven Hundred Fifty Dollars and Zero Cents (\$1,750.00) for the Class Representatives. To the extent more than \$1,750.00 service awards are sought for the Class Representatives, PRGX has reserved all rights to object and oppose such a request.

EXCLUDING YOURSELF FROM THE SETTLEMENT

16. How do I opt out of the Settlement?

If you do not want to receive any benefits from the Settlement, and you want to keep your right, if any, to separately sue the Defendant about the legal issues in this case, you must take steps to exclude yourself from the Settlement Class. This is called "opting out" of the Settlement Class. The deadline for requesting exclusion from the Settlement is **[Deadline Date]**.

To exclude yourself from the Settlement, you must submit a written request for exclusion that includes the following information:

- *Ebert, et al. v. PRGX Global, Inc.*, Case No. 1:23-cv-04233-TWT, U.S.D.C. Northern District of Georgia – Atlanta Division;
- your full name;
- current address;
- personal signature; and
- the words "Request for Exclusion" or a comparable statement that you do not wish to participate in the Settlement.

Your request for exclusion must be mailed to the Settlement Administrator at the address below, postmarked no later than **[Deadline Date]**.

PRGX Data Incident Settlement Administrator
ATTN: Exclusion Request
P.O. Box 58220
Philadelphia, PA 19102

If you exclude yourself, you are telling the Court that you do not want to be part of the Settlement. You will not be eligible to receive a payment or any other benefits under the Settlement if you exclude yourself. You may only exclude yourself – not any other person.

COMMENTING ON OR OBJECTING TO THE SETTLEMENT

17. How do I tell the Court if I like or do not like the Settlement?

If you are a Settlement Class Member, you can choose (but are not required) to object to the Settlement if you do not like it or a portion of it. You can give reasons why you think the Court should not approve the Settlement.

For an objection to be considered by the Court, the objection must include: (i) the name of the proceedings; (ii) the Settlement Class Member's full name, current mailing address, and telephone number; (iii) a statement that states with specificity the grounds for the objection, as well as any documents supporting the objection; (iv) a statement as to whether the objection applies only to the objector, to a specific subset of the Settlement Class, or to the entire Settlement Class; (v) the identity of any attorneys representing the objector; (vi) a statement regarding whether the Settlement Class Member (or his/her attorney) intends to appear at the Final Approval Hearing; (vii) a list of all other matters in which the objecting Settlement Class Member and/or his/her attorney has lodged an objection to a class action settlement; and (viii) the signature of the Settlement Class Member or the Settlement Class Member's attorney.

Any Settlement Class Member who does not file a timely and adequate objection in accordance with above paragraph waives the right to object or to be heard at the Final Approval Hearing and will be forever barred from making any objection to the Settlement and will be bound by the terms of the Agreement and by all proceedings, orders, and judgments in the Action.

Objections must be filed with the Court no later than **[Deadline Date]**.

Clerk of the Court
2188 Richard B. Russell Federal Building and United States Courthouse
75 Ted Turner Drive, SW
Atlanta, GA 30303-3309

18. What is the difference between objecting and excluding?

Objecting is telling the Court that you do not like something about the Settlement. You can object to the Settlement only if you do not exclude yourself from the Settlement. Excluding yourself from the Settlement is opting out and stating to the Court that you do not want to be part of the Settlement. If you opt out of the Settlement, you cannot object to it because the Settlement no longer affects you.

THE COURT'S FINAL APPROVAL HEARING

19. When is the Court's Final Approval Hearing?

The Court is scheduled to hold a final approval hearing on _____, 2024 at _____ a.m./p.m. E.T., at [address/via zoom], Courtroom _____, to decide whether to approve the Settlement, how much attorneys' fees and costs to award to Settlement Class Counsel for representing the Settlement Class, and whether to award a service award payment to each Class Representative who brought this Action on behalf of the Settlement Class. If you are a Settlement Class Member, you or your attorney may ask permission to speak at the hearing at your own cost. The date and time of this hearing may change without further notice. Please check [www._____](http://www._____.) for updates.

20. Do I have to come to the Final Approval Hearing?

No. Settlement Class Counsel will answer any questions the Court may have. You may attend at your own expense if you wish. If you file an objection, you do not have to come to the Final Approval Hearing to talk about it. If you file your written objection on time and in accordance with the requirements above, the Court will consider it. You may also pay your own lawyer to attend, but such attendance is not necessary for the Court to consider an objection that was filed on time and meets the requirements above.

IF I DO NOTHING

21. What happens if I do nothing at all?

If you are a Settlement Class Member and you do nothing, you will give up the rights explained in **Question 9**, including your right to start a lawsuit, continue a lawsuit, or be part of any other lawsuit against the Defendant and the Released Parties, as defined in the Settlement Agreement, about the legal issues resolved by this Settlement. In addition, you will not receive a payment from this Settlement.

GETTING MORE INFORMATION

22. How do I get more information?

This Notice summarizes the proposed Settlement. Complete details are provided in the Settlement Agreement. The Settlement Agreement and other related documents are available at the Settlement Website, [\[Website URL\]](#).

If you have additional questions, you may contact the Settlement Administrator by email, phone, or mail:

Email: [\[Email Address\]](#)

Toll-Free: 1-[XXX-XXX-XXXX](#)

Mail: PRGX Data Incident, c/o Settlement Administrator, 1650 Arch Street, Suite 2210, Philadelphia, PA 19103

Publicly filed documents can also be obtained by visiting the office of the United States District Court for the Northern District of Georgia, Atlanta Division, or by reviewing the Court's online docket.

PLEASE DO NOT CONTACT THE COURT OR PRGX

Exhibit D

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

Jeffrey Ebert, on behalf of himself and on behalf of his minor children **M.E., E.E., and S.E.**, and **Jennifer Ebert**, on behalf of herself, and collectively on behalf of all others similarly situated,

Plaintiffs,

v.

PRGX Global, Inc.,

Defendant.

Case No. 1:23-CV-04233-TWT

JURY TRIAL DEMANDED

SECOND AMENDED CLASS ACTION COMPLAINT

Plaintiff Jeffrey Ebert, individually and on behalf of his minor children M.E., E.E., and S.E., and Plaintiff Jennifer Ebert (“Plaintiffs”), individually, and collectively on behalf of all other similarly situated individuals (the “Class” or “Class Members,” as defined below), by and through their undersigned counsel, file this Second Amended Class Action Complaint against PRGX Global Inc., a Georgia corporation (“PRGX” or “Defendant”) and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of counsel as to all other matters.

I. NATURE OF THE ACTION

1. Founded in 1970, PRGX is a business services company based in Atlanta, Georgia.¹

2. PRGX provides global recovery audit and spend analytics services and consulting services to companies in the media, banking, telecom, utilities, oil and gas, manufacturing, retail, and consumer goods industries.²

3. PRGX employs more than 1,500 people and generates approximately \$41 million in annual revenue.³

4. In the ordinary course of business, PRGX receives the personally identifiable information (“PII”) and protected health information (“PHI”) of individuals, such as Plaintiffs and the Class, from the clients PRGX services and through the employees PRGX hires.

5. PRGX obtains, collects, uses, and derives a benefit from the PII/PHI of Plaintiffs’ and Class Members. PRGX uses the PII/PHI it collects to provide services to its clients, making a profit therefrom. By doing so, PRGX assumed the legal and equitable duties to those individuals to protect and safeguard their PII/PHI from

¹ See <https://www.jdsupra.com/legalnews/prgx-global-inc-notifies-13-231-2850522/>.

² *Id.*

³ *Id.*

unauthorized access and intrusion.

6. Plaintiffs and the Class Members (as further defined below) have had their PII and/or PHI exposed as a result of PRGX's inadequately secured computer network.

7. On May 5, 2023, PRGX disclosed, for the first time, a data security incident that took place between April 8, 2022, and April 9, 2022, in which cybercriminals were able to access the PII of approximately **13,231 individuals** (the "Data Breach," or the "Breach").⁴ The types of PII/PHI compromised included names; dates of birth; Social Security numbers; driver's license numbers; credit card information; financial account information; health insurance information; medical information; electronic signatures; employer assigned identification numbers; passport numbers; and online usernames and passwords (collectively, "Private Information"). This class action seeks to redress PRGX's unlawful, willful and wanton failure to protect the PII Plaintiffs and the Class.

8. The Data Breach was discovered on April 9, 2022, when PRGX learned that certain servers and systems in its environment were inaccessible.⁵

⁴ See <https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml>.

⁵ See Notice Letters of Plaintiffs, attached hereto as Exhibits 1–5.

9. PRGX launched an investigation with the assistance of third-party computer specialists, which confirmed an unknown actor “took or viewed certain files.”⁶

10. Despite learning of the Data Breach on April 9, 2022, PRGX did not notify victims of the Data Breach until on or around May 5, 2023, over a year after the Data Breach occurred.⁷

11. Defendant sent out notice of data breach letters (“Notice Letters”) to victims of the Data Breach in or around May 2023.

12. After the Data Breach, several sources, like the one pictured below, reported Black Basta Group (“Black Basta”), a well-known criminal ransomware group, was responsible for the Breach:⁸

[IMAGE ON FOLLOWING PAGE]

⁶ *Id.*

⁷ *Id.*

⁸ See *Black Basta Ransomware Victim: PRGX Global Inc[.],* REDPACKET SECURITY, <https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/>; *Weekly Dark Web Trends/Advisory*, CYFIRMA, available at https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf; *Profiles for ransomware group: blackbasta*, RANSWOMWARE.LIVE, <https://www.ransomware.live/#/group/blackbasta>; RANSOMLOOK, <https://www.ransomlook.io/search> (input “PRGX” in the search bar).

Victim Name	PRGX Global Inc.
Victim URL	hXXps://stniomyjliimcgkvdsvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion/?id=PRGX Global Inc.
Description	Building on our deep recovery audit expertise, we develop and deploy industry-leading solutions that help clients mine their data to reduce cost, optimize working capital and mitigate risk in their Source-to-Pay processes. With unmatched experience and expertise in data analysis, PRGX is uniquely qualified to help our clients improve performance across all variables in the Source-to-Pay process. We can quickly and rigorously aggregate large amounts of complex data from disparate sources; apply advanced analytics to the data, uncovering actionable insights; and implement strategies that eliminate costly leakage and improve profitability.
Percent of Leaked Files (at time of posting)	100%
Number of Times Victim Post has been viewed	3699

13. “Like other enterprise-targeting ransomware operations, Black Basta will steal corporate data and documents before encrypting a company's devices. This stolen data is then used in double-extortion attacks, where the threat actors demand a ransom to receive a decryptor and prevent the publishing of the victim's stolen data. The data extortion part of these attacks is conducted on the 'Black Basta Blog' or 'Basta News' Tor site, which contains a list of all victims who have not paid a ransom. Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom.”⁹

⁹ Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM),

14. Black Basta’s “encryption algorithm is secure and [] there is no way to recover files for free.”¹⁰

15. Plaintiffs and the Class were left in the dark for over a year regarding the theft of their Private Information and whether PRGX was able to retrieve it.

16. PRGX has offered no assurance it paid Black Basta’s ransom demand to retrieve Plaintiffs’ and the Class’s Private Information and prevent it from being posted on the dark web.

17. Even if PRGX did pay Black Basta’s ransom demand that does not mean Black Basta will not post and/or sell Plaintiffs’ and the Class’s Private Information on the dark web in the future, doubling its profits. After all, Black Basta is known to be a “financially motivated” ransomware group.¹¹

<https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>; *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

¹⁰ Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.

¹¹ *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), *available at* <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

18. Due to Defendant's negligence, cybercriminals obtained everything they needed to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

19. Now, for the rest of their lives, Plaintiffs and Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

20. Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

21. Plaintiff **Jeffrey Ebert** is an individual domiciled in Arizona. On or about May 5, 2023, Defendant sent Plaintiff Jeffrey Ebert a Notice Letter informing

him that his name and Social Security number were compromised in the Data Breach.

22. Plaintiff **Jennifer Ebert** is an individual domiciled in Arizona. On or about May 5, 2023, Defendant sent Plaintiff Jennifer Ebert a Notice Letter informing her that her name and Social Security number were compromised in the Data Breach.

23. Plaintiff Jeffrey Ebert and Plaintiff Jennifer Ebert are the parents of minor children **M.E., S.E., and E.E.** (the “Minor Plaintiffs”) who are also domiciled in Arizona. On or about May 5, 2023, Defendant sent Notice Letters “to the parent or guardian of” the Minor Plaintiffs informing them that the Minor Plaintiffs’ names and Social Security numbers were compromised in the Data Breach.

24. Defendant **PRGX** is a Georgia corporation with its principal place of business located at 200 Galleria Pkwy, Suite 450, Atlanta, GA, 30339. Defendant maintains and transacts business across the state of Georgia.

III. JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (“CAFA”), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of \$5,000,000.00 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

26. This Court has personal jurisdiction over Defendant because Defendant is incorporated and/or has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

27. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. PRGX's Data Breach

28. In the ordinary course of business, PRGX receives the Private Information of individuals, such as Plaintiffs and the Class, from the employees PRGX hires and from the clients PRGX services.

29. PRGX obtains, collects, uses, and derives a benefit from the Private Information of Plaintiffs' and Class Members. PRGX uses the Private Information it collects to provide services to its clients, making a profit therefrom. PRGX would not be able to obtain revenue if not for the acceptance and use of Plaintiffs' and the Class's Private Information.

30. By collecting Plaintiffs' and the Class's Private Information, PRGX assumed legal and equitable duties to Plaintiffs and the Class to protect and

safeguard their Private Information from unauthorized access and intrusion.

31. PRGX recognizes this duty and makes the following claim on its website regarding its protection of sensitive data: “Ingesting, analyzing and storing data securely for complete privacy, control and transparency, meeting or exceeding all relevant laws, regulations and industry best practices.”¹²

32. However, PRGX failed to protect Plaintiffs’ and the Class’s Private Information.

33. As a result, Plaintiffs’ and Class Members’ Private Information was accessed and stolen from PRGX’s inadequately secured computer network in a massive and preventable data breach, as corroborated by the source below:¹³

[IMAGE ON FOLLOWING PAGE]

¹² See *Technology Platforms*, PRGX, <https://www.prgx.com/technology-platforms/>.

¹³ RANSOMLOOK, <https://www.ransomlook.io/search> (input “PRGX” in the search bar).

Posts		
Group	Title	Date
Blackbasta	PRGX Global Inc.	2022-08-18
Clop	PRGX.COM	2023-07-15
Clop Torrents	prgx.com	2023-08-27
FULL FILES magnet: xt=urn:btih:b4f58ca8706b9f8472d470294444fa2796e664e1&dn=prgx		

34. On April 9, 2022, PRGX noticed that certain computer servers and systems in its environment were inaccessible.¹⁴

35. After an investigation, PRGX determined cybercriminals infiltrated PRGX's network and gained unauthorized access to certain files between April 8, 2022, and April 9, 2022.¹⁵

36. Specifically, PRGX admits the unauthorized actor(s) “**took or viewed certain files.**”¹⁶

37. The Private Information stolen in the Data Breach included names;

¹⁴ See Exhibits 1–5.

¹⁵ *Id.*

¹⁶ *Id.* (emphasis added).

dates of birth; Social Security numbers; driver's license numbers; credit card information; financial account information; health insurance information; medical information; electronic signatures; employer assigned identification numbers; passport numbers; and online usernames and passwords.¹⁷

38. Despite discovering the Data Breach on April 9, 2022, PRGX took over a year to notify victims of the Data Breach that their information was viewed and stolen, giving cybercriminals a more than a 365-day head start on misusing and exploiting Plaintiffs' and the Class's Private Information.

39. In recognition of the severity of the Data Breach, and the imminent risk of impending harm Plaintiffs and the Class face, PRGX made an offering of twelve (12) months of credit monitoring and identity restoration services through IDX to victims of the Data Breach. Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has already occurred.

40. All in all, PRGX failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

¹⁷ See *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, <https://apps.web.maine.gov/online/aevier/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml>.

41. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

42. Shortly after the Data Breach, various sources reported criminal ransomware group, Black Basta, was responsible for the Data Breach.¹⁸

43. Black Basta is a "financially motivated"¹⁹ criminal ransomware group who is "aggressive and highly active."²⁰

44. Black Basta is "known for its double extortion attack"²¹ and has

¹⁸ See *Black Basta Ransomware Victim: PRGX Global Inc[.]*, REDPACKET SECURITY, <https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/>; *Weekly Dark Web Trends/Advisory*, CYFIRMA, available at https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf; *Profiles for ransomware group: blackbasta*, RANSWOMWARE.LIVE, <https://www.ransomware.live/#/group/blackbasta>; RANSOMLOOK, <https://www.ransomlook.io/search> (input "PRGX" in the search bar).

¹⁹ *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), available at <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

²⁰ *Black Basta, Anatomy of the Attack*, INFOBLOX (May 19, 2023) <https://blogs.infoblox.com/cyber-threat-intelligence/black-basta-anatomy-of-the-attack/>.

²¹ *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), available at <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

“proven itself to be a formidable threat.”²²

45. Like other ransomware gangs, Black Basta steals corporate data and documents before it encrypts the information.²³

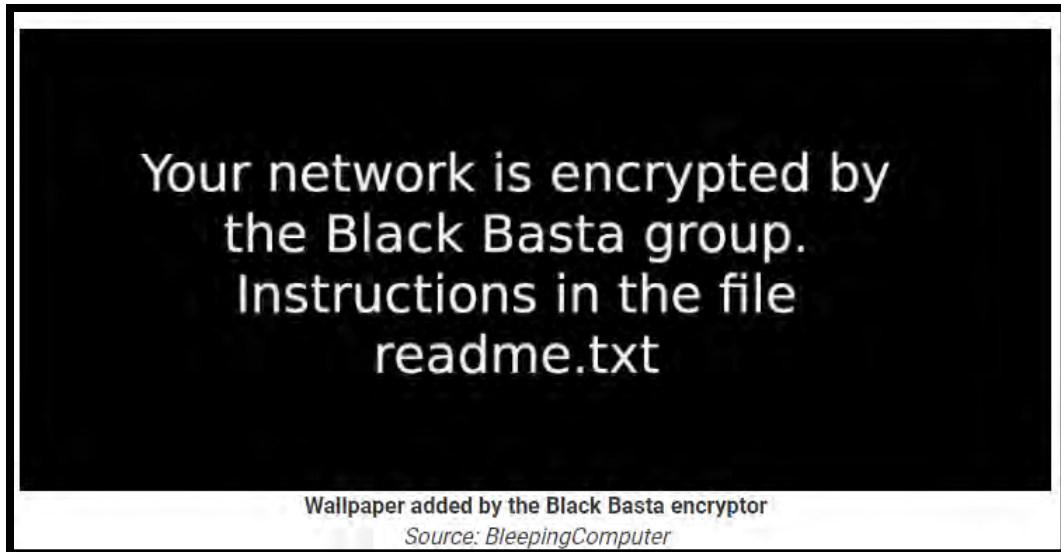
46. “Once the encryption process is complete, the malware changes the wallpaper, and files on the desktop become encrypted and unusable,” as pictured below:²⁴

[IMAGE ON FOLLOWING PAGE]

²² *Ransomware Spotlight Black Basta*, TREND MICRO INCORPORATED (Sept. 1, 2022), <https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta>.

²³ Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.

²⁴ *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), available at <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>; Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.



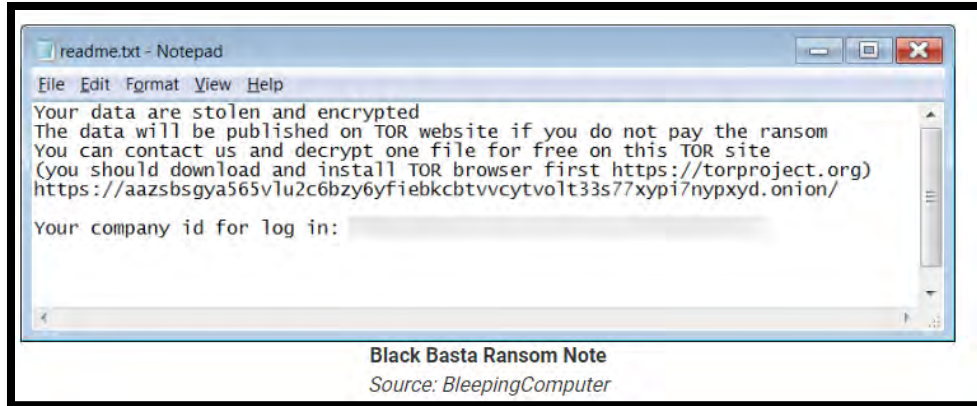
47. Black Basta then demands a hefty ransom from the company it steals the information from in exchange for a decryptor, which will allow the company to access its files again.²⁵

48. Below is the ransom note Black Basta typically uses.²⁶

[IMAGE ON FOLLOWING PAGE]

²⁵ Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.

²⁶ *Id.*



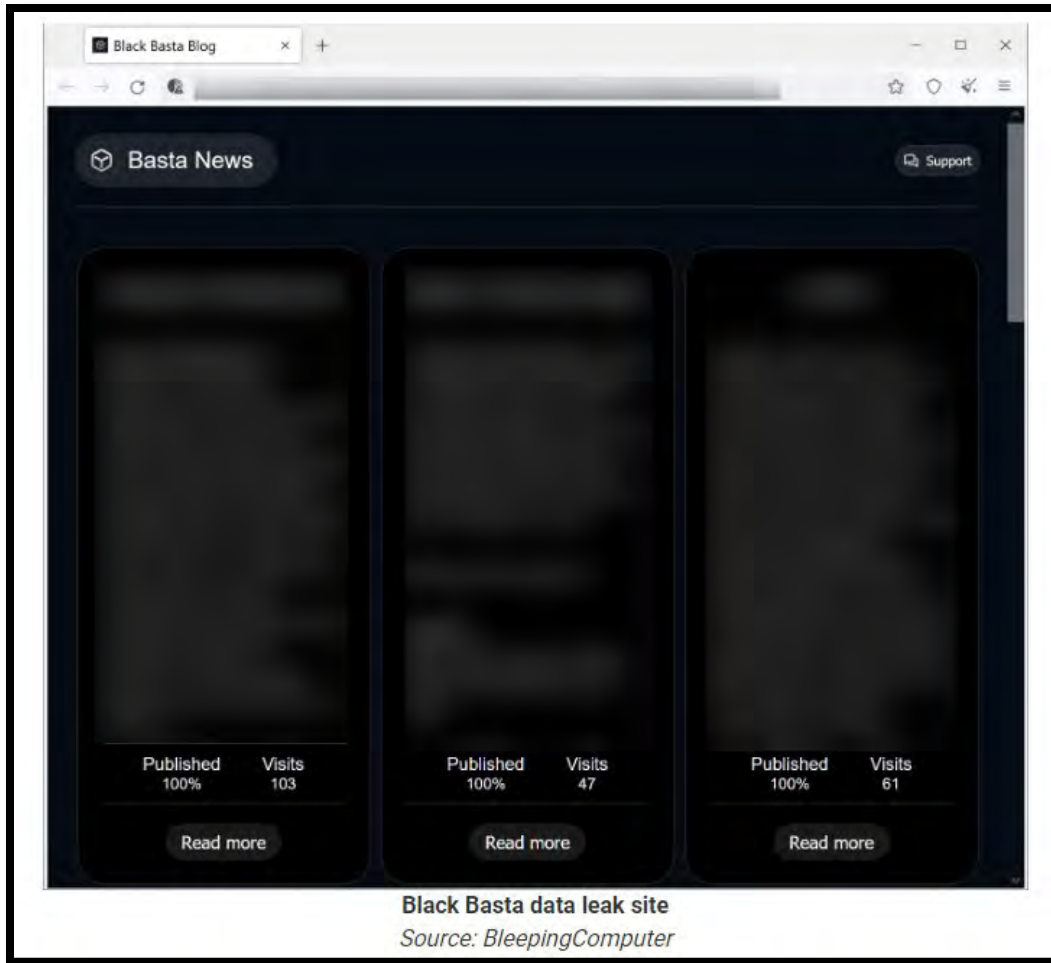
49. Black Basta “not only executes ransomware, but also exfiltrates sensitive data, operating a cybercrime marketplace to publicly release it, should a victim fail to pay a ransom.”²⁷

50. Black Basta “deploys a name-and-shame approach to their victims, using a Tor site, Basta News, to publicly list victims’ names, descriptions, percentage of published data stolen, number of visits, and any other data exfiltrated [sic].”²⁸

[IMAGE ON FOLLOWING PAGE]

²⁷ *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023), available at <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

²⁸ *Id.*; Amer Elsad, *Threat Assessment: Black Basta Ransomware*, UNIT 42 (Aug. 25, 2022 12:00 PM) <https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/>.



51. “Black Basta will slowly leak data for each victim to try and pressure them into paying a ransom.”²⁹

52. As evidenced below, a source claims Black Basta already deployed its

²⁹ Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>.

signature approach here:³⁰

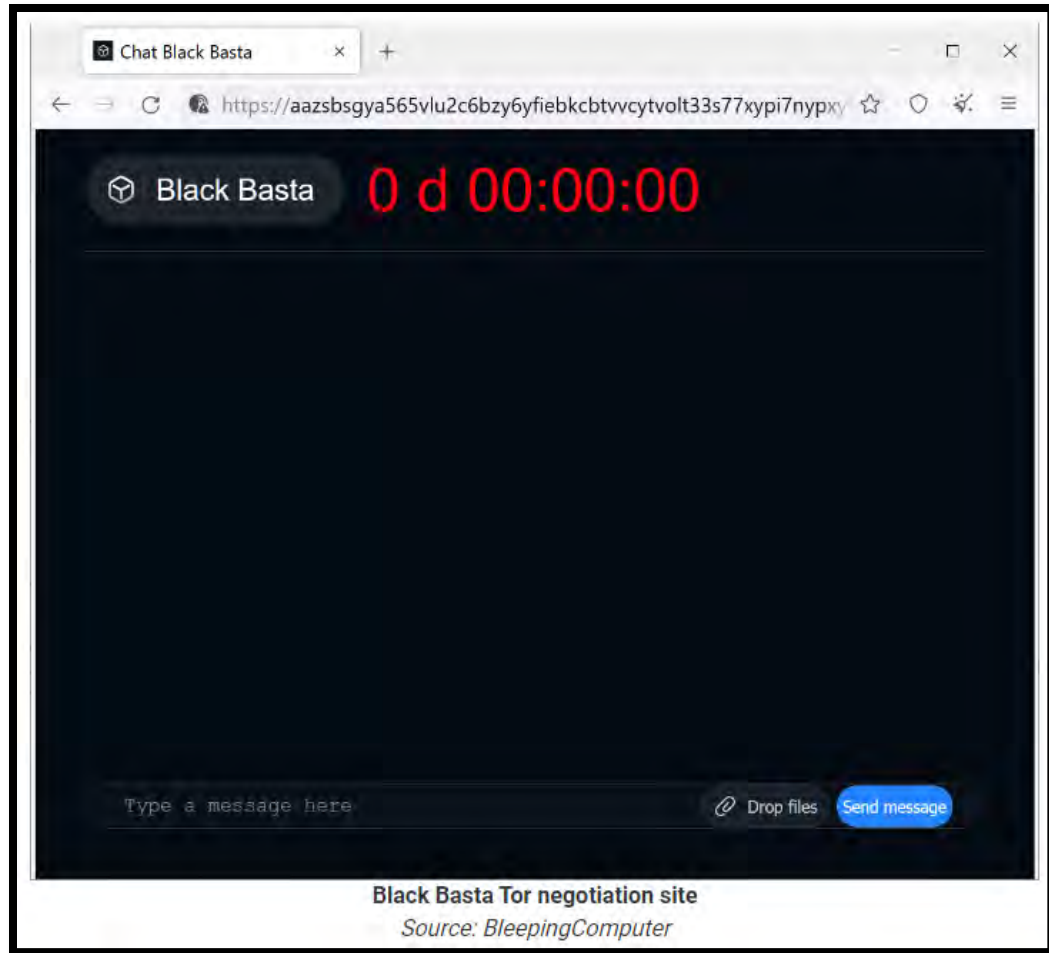
Victim Name	PRGX Global Inc.
Victim URL	hXXps://stniiomyjliimcgkvdszvgen3eaaoz55hreqqx6o77yvmpwt7gklffqd[.]onion/?id=PRGX Global Inc.
Description	Building on our deep recovery audit expertise, we develop and deploy industry-leading solutions that help clients mine their data to reduce cost, optimize working capital and mitigate risk in their Source-to-Pay processes. With unmatched experience and expertise in data analysis, PRGX is uniquely qualified to help our clients improve performance across all variables in the Source-to-Pay process. We can quickly and rigorously aggregate large amounts of complex data from disparate sources; apply advanced analytics to the data, uncovering actionable insights; and implement strategies that eliminate costly leakage and improve profitability.
Percent of Leaked Files (at time of posting)	100%
Number of Times Victim Post has been viewed	3699

53. Black Basta will leak the data it steals if the ransom demand is not paid:³¹

[IMAGE ON FOLLOWING PAGE]

³⁰ See *Black Basta Ransomware Victim: PRGX Global Inc[.]*, REDPACKET SECURITY, <https://www.redpacketsecurity.com/black-basta-ransomware-victim-prgx-global-inc/> (reporting dark web findings).

³¹ See Lawrence Abrams, *New Black Basta ransomware spring into action with a dozen breaches*, BLEEPINGCOMPUTER (April 27, 2022, 5:46 PM), <https://www.bleepingcomputer.com/news/security/new-black-basta-ransomware-springs-into-action-with-a-dozen-breaches/>; *Weekly Dark Web Trends/Advisory*, CYFIRMA, available at https://www.prianto.com/fileadmin/user_upload/PRIANTO_CEE/Cyfirma/Weekly_Dark_Web_Trends_and_Advisory_13_May_2022.pdf.



54. PRGX makes no assurances to Plaintiffs and the Class that it attempted to regain Plaintiffs' and the Class's data from Black Basta, paid the ransom demand, or that their data has not already been posted on the dark web.

55. Even if PRGX did pay the ransom this does not mean that Black Basta will not exploit Plaintiffs' and the Class's Private Information in the future for further financial gain or has not already done so. After all, Black Basta is a

“financially motivated” group of criminals.³²

56. Plaintiffs and the Class reasonably believe their data is on the dark web or has already been sold/exploited on the dark web because: (i) PRGX failed to prevent the Data Breach; (ii) the cybergang believed to have perpetrated the Breach, Black Basta, is known to leak stolen Private Information on the dark web; (iii) Defendant has not provided any assurance that it paid a ransom to the cybercriminals to prevent Plaintiffs’ and the Class’s data from being released on the dark web; and (iv) Defendant offered credit monitoring to Plaintiffs and the Class, an offer it need not make if no Private Information was stolen and at risk of misuse.

57. As such, Plaintiffs and the Class are at an imminent and impending risk of fraud and identity theft for the rest of their lives and seek relief from PRGX.

B. Cybercriminals Will Use Plaintiffs’ Private Information to Defraud Them.

58. Private Information is of great value to hackers and cybercriminals, and the Private Information stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

³² *HC3 Threat Profile*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES HEALTH SECTOR CYBERSECURITY COORDINATION CENTER (Mar. 15, 2023) *available at* <https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf>.

59. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.³³ For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.³⁴ These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

60. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

Social Security number. *This is the most dangerous type of personal information in the hands of identity thieves because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal*

³³ “Facts + Statistics: Identity Theft and Cybercrime,” Insurance Info. Inst., <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime> (discussing Javelin Strategy & Research’s report “2018 Identity Fraud: Fraud Enters a New Era of Complexity”).

³⁴ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.³⁵

[Emphasis added.]

61. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.³⁶

62. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like PRGX is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for \$60 to \$80 on the digital black market.³⁷ “[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web.”³⁸

³⁵ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

³⁶ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at <https://www.gao.gov/products/gao-07-737>.

³⁷ Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, <https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web>.

³⁸ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

63. These risks are both certainly impending and substantial. As the Federal Trade Commission (“FTC”) has reported, if hackers get access to Private Information, they will use it.³⁹

64. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁴⁰

65. For instance, with a stolen social security number, which is part of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.⁴¹

³⁹ Ari Lazarus, *How fast will identity thieves use stolen info?*, Military Consumer, May 24, 2017, <https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info>.

⁴⁰ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at <https://www.gao.gov/products/gao-07-737>.

⁴¹ See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

66. Identity theft victims like Plaintiffs as well as other Class Members, must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.⁴²

67. Defendant's offer of one (1) year of identity monitoring to Plaintiffs and the Class is woefully inadequate and will not fully protect Plaintiffs from the damages and harm caused by its failures. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Once the coverage has expired, Plaintiffs and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to PRGX's gross negligence.

68. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information)—it does not prevent identity theft.⁴³ Nor can an identity monitoring service remove personal information from the dark

⁴² "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), available at <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

⁴³ See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, <https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html>.

web.⁴⁴ “The people who trade in stolen personal information [on the dark web] won’t cooperate with an identity theft service or anyone else, so it’s impossible to get the information removed, stop its sale, or prevent someone who buys it from using it.”⁴⁵

69. As a direct and proximate result of the Data Breach, Plaintiffs and/or the Class have suffered actual identity theft, have been damaged, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft.

70. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

71. Even more seriously is the identity restoration that Plaintiffs and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver’s license replacement applications, and calling

⁴⁴ *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

⁴⁵ *Id.*

financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiffs and the Class must take.

72. Plaintiffs and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

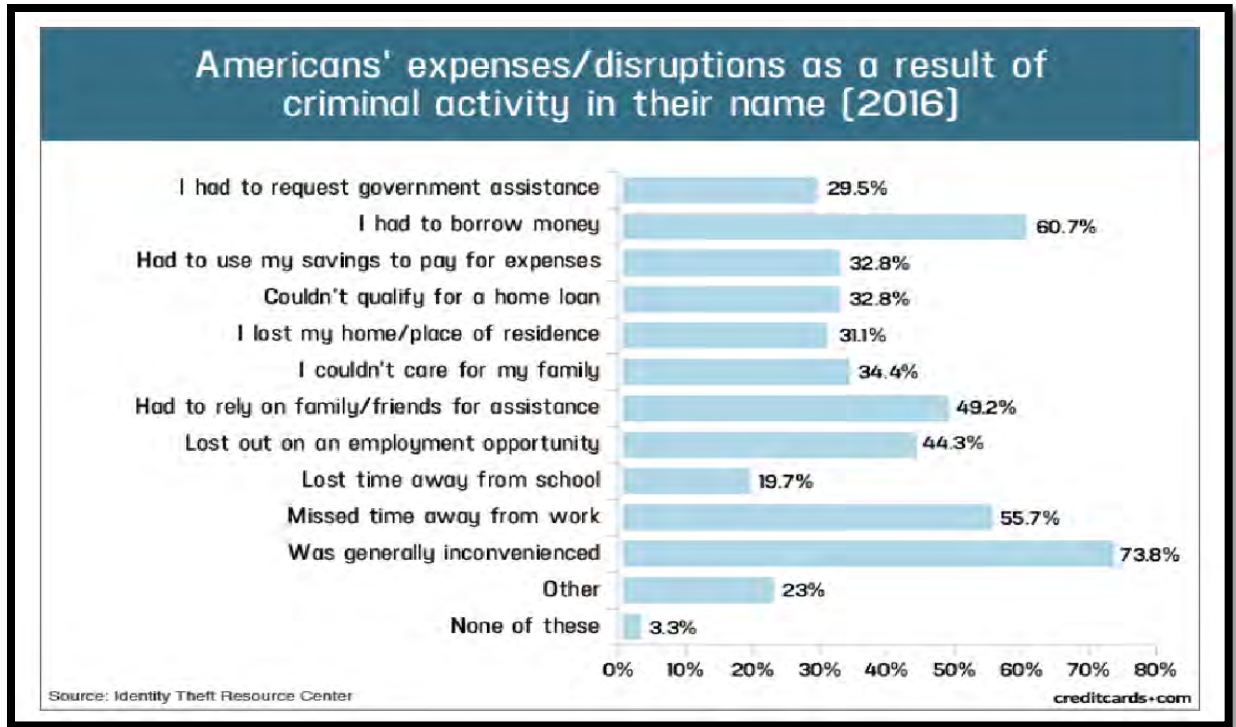
- a. Actual identity theft;
- b. Trespass, damage to, and theft of their personal property including Private Information;
- c. Improper disclosure and/or theft of their Private Information;
- d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;
- e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their Private Information;
- f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;
- g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

- h. Ascertainable losses in the form of deprivation of the value of Plaintiffs' and Class members' Private Information for which there is a well-established and quantifiable national and international market;
- i. The loss of use of and access to their credit, accounts, and/or funds;
- j. Damage to their credit due to fraudulent use of their Private Information; and/or
- k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

73. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience⁴⁶:

[CHART ON FOLLOWING PAGE]

⁴⁶ Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), <https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/>.



74. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiffs' and the Class's Private Information.

75. Plaintiffs and Class Members also have an interest in ensuring that their Private Information that was provided to PRGX is removed from all PRGX servers, systems, and files.

76. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members the woefully inadequate twelve (12) months of identity theft repair and monitoring services. Twelve (12) months of

identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

77. Defendant further acknowledged, in its letter to Plaintiffs and other Class Members, that PRGX needed to improve its security protocols, stating: “while we have safeguards in place to protect data in our care, we have taken steps to further enhance these protections and continue to monitor these safeguards as part of our ongoing commitment to data security.”⁴⁷

78. The letter further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: “We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors.”⁴⁸

79. At PRGX’s suggestion, Plaintiffs are desperately trying to mitigate the damage that PRGX has caused them. Given the kind of Private Information PRGX made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of

⁴⁷ See Notice Letters of Plaintiffs, attached hereto as Exhibits 1–5.

⁴⁸ *Id.*

their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.⁴⁹

80. None of this should have happened, the Data Breach was entirely preventable.

C. Defendant was Aware of the Risk of Cyberattacks

81. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,⁵⁰ Yahoo,⁵¹

⁴⁹ *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

⁵⁰ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>.

⁵¹ Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html>.

Marriott International,⁵² Chipotle, Chili's, Arby's,⁵³ and others.⁵⁴

82. PRGX should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the Private Information that it collected and maintained.

83. Indeed, PRGX's Privacy Policy⁵⁵ states in pertinent part as follows:

How We Protect Personal Information We Process on Behalf of Our Clients

PRGX is a business-to-business information and professional services firm that collects and processes transactional client data for improving clients' financial performance by reducing costs, improving business processes and increasing profitability. PRGX's core business segment is recovery audit services which is the processing of source-to-pay transactional information (e.g., accounts payable data, vendor file information and line item/product data) to identify client overpayments made to their third-party suppliers or vendors. Other

⁵² Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), <https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/>.

⁵³ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), <https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b>.

⁵⁴ See, e.g., Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

⁵⁵ <https://www.prgx.com/privacy-policy/#:~:text=PRGX%20is%20committed%20to%20protecting,internal%20policies%2C%20practices%20and%20procedures.>

business segments include providing analytics and advisory services to senior financial executives.

We process this transactional information on behalf of our clients to perform the requested services. This transactional information may contain Personal Information in limited circumstances, such as when a client's third-party supplier or vendor happens to be a sole proprietor. Information on these individuals is used and processed as instructed by our clients for accounts payable recovery auditing or other requested services in accordance with client contractual requirements. In any event, regarding transactional information that constitutes Personal Information, we act in a data processor capacity, meaning we collect and process this Personal Information only as instructed by our client and will not use or disclose it for our own purposes.

We do, however, maintain information security controls to protect this Personal Information and will only disclose or transfer this information as instructed by or agreed upon with our client to provide the requested service. Unless otherwise instructed by our clients, we treat the Personal Information we process on behalf of our clients in line with our commitments on disclosure and transfer as set forth in this Statement.

* * *

Security And Data Integrity

PRGX is committed to protecting the privacy, confidentiality, and security of the data that is provided to us, including Personal Information, through a combination of technical, physical and administrative controls, including internal policies, practices and procedures.

We apply appropriate technical, physical and organizational measures that are reasonably designed to protect Personal Information against accidental or

unlawful destruction, loss, alteration, unauthorized disclosure or access where Personal Information is transferred over a network, and against all other unlawful forms of processing. Access to Personal Information is restricted to authorized recipients on a need-to-know basis. We maintain a comprehensive information security program that is proportionate to the risks associated with the processing. The program is continuously adapted to mitigate operational risks and to ensure the protection of Personal Information taking into account industry-accepted practices. We will also use enhanced security measures in case we process any Sensitive Personal Information.

PRGX's privacy and security framework is based on ISO 27001 standards and, as such, we have a strong focus on establishing, maintaining, and continuously improving information security management systems and identifying, analyzing, and addressing information security risks. The ISO 27001 standards cover all aspects of security including physical protection of equipment and people, hiring practices, employee training, network security, and access controls. This framework combined with regular monitoring and testing of controls, allows us to ensure that appropriate levels of data confidentiality, integrity, and availability are maintained.

84. PRGX's assurances of maintaining high standards of cybersecurity make it evident that PRGX recognized it had a duty to use reasonable measures to protect the Private Information that it collected and maintained.

85. PRGX was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

D. PRGX Could Have Prevented the Data Breach.

86. Data breaches are preventable.⁵⁶ As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions.”⁵⁷ She added that “[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised”⁵⁸

87. “Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*.”⁵⁹

88. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security

⁵⁶ Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are Preventable,” in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at <https://lawcat.berkeley.edu/record/394088>.

⁵⁷*Id.* at 17.

⁵⁸*Id.* at 28.

⁵⁹*Id.*

practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.⁶⁰ The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

89. According to information and belief, PRGX failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines.

90. Upon information and belief, PRGX also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and

⁶⁰ FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

91. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁶¹

92. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

⁶¹ See *How to Protect Your Networks from RANSOMWARE*, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁶²

93. Further, to prevent and detect malware attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

⁶² *Id.* at 3–4.

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website’s security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them

updated—to reduce malicious network traffic....⁶³

94. In addition, to prevent and detect ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
 - Apply latest security updates
 - Use threat and vulnerability management
 - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
 - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
 - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
 - Use [multifactor authentication] or [network level

⁶³ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at <https://www.cisa.gov/news-events/news/protecting-against-ransomware>.

authentication] and use strong, randomized, just-in-time
local admin passwords

- **Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

- **Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].⁶⁴

⁶⁴ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

95. Given that Defendant was storing the Private Information of more than 13,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

96. Specifically, among other failures, PRGX had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.⁶⁵

97. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed. The FTC, among others, has repeatedly emphasized the importance of disposing of unnecessary Private Information, saying simply: “Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁶⁶ PRGX, rather than following this basic standard of care, kept thousands of individuals unencrypted Private Information indefinitely.

⁶⁵ See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.

⁶⁶ FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

98. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all Private Information. Further, the scope of the Data Breach could have been dramatically reduced had PRGX utilized proper record retention and destruction practices.

E. PRGX’s Response to the Data Breach is Inadequate to Protect Plaintiffs and the Class.

99. PRGX failed to timely inform Plaintiffs and Class Members of the Data Breach.

100. PRGX stated that it discovered the Data Breach on April 9, 2022. And yet, PRGX did not start notifying affected individuals until May 5, 2023—over one (1) year after it learned of the Data Breach.

101. During these intervals, the cybercriminals were exploiting the information while PRGX was secretly still investigating the Data Breach.

102. If PRGX had investigated the Data Breach more diligently and reported it sooner, Plaintiffs’ and the Class’s damages could have been mitigated.

F. Plaintiffs’ Individual Experiences.

Plaintiff Jeffrey Ebert’s Experience and the Minor Plaintiffs’ Experiences

103. Plaintiff Jeffrey Ebert is a former employee of Defendant. Plaintiff Jeffrey Ebert agreed to entrust his Private Information and the Minor Plaintiffs’ Private Information to Defendant as a condition of receiving employment and/or elective benefits. In exchange, Defendant agreed not only to accept this Private

Information, but also to safeguard it and delete it after a reasonable time following the termination of the employment relationship. Plaintiff Jeffrey Ebert did not reasonably expect that he was providing his and the Minor Plaintiffs' Private Information to Defendant forever.

104. Defendant was in possession of Plaintiff Jeffrey Ebert's Private Information and the Minor Plaintiffs' Private Information before, during, and after the Data Breach.

105. In or around May 2023, Plaintiff Jeffrey Ebert and the Minor Plaintiffs received Notice Letters from Defendant informing them that they were victims of the Data Breach and that an unauthorized actor "took or viewed certain files" in the Data Breach, including their Private Information.

106. As a direct and traceable result of the Data Breach, Plaintiff Jeffrey Ebert has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach, reviewing, and monitoring his accounts for fraudulent activity, reviewing his credit reports, and/or researching credit monitoring services. However, this is not the end. Plaintiff Jeffrey Ebert, the Minor Plaintiffs, and Class Members will be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant's direction, which has been lost forever and cannot be recaptured.

107. Plaintiff Jeffrey Ebert and the Minor Plaintiffs place significant value in the security of their Private Information and do not readily disclose it. Plaintiff Jeffrey Ebert entrusted his Private Information and the Minor Plaintiffs' Private Information to Defendant with the understanding that Defendant would keep this information secure and would employ reasonable and adequate security measures to ensure that their Private Information would not be compromised.

108. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

109. As a direct and traceable result of the Data Breach, Plaintiff Jeffrey Ebert and/or the Minor Plaintiffs suffered actual damages such as: (1) lost time related to monitoring their accounts and credit reports for fraudulent activity; (2) loss of privacy due to their Private Information being exposed to cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect their Private Information; (4) exposure to increased and imminent risk of fraud and identity theft now that their Private Information has been exposed; (5) the loss in value of their Private Information due to their Private Information being in the hands of cybercriminals who can use it at their leisure; and/or (6) other economic and non-economic harm.

110. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have been and will

continue to be at a heightened and substantial risk of future identity theft and its attendant damages for *years* to come, especially the Minor Plaintiffs. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class.

111. Plaintiff Jeffrey Ebert and the Minor Plaintiffs have a continuing interest in ensuring that their Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiffs', and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Jennifer Ebert's Experience

112. Plaintiff Jennifer Ebert is the spouse of Jeffrey Ebert, and the mother of the Minor Plaintiffs. Plaintiff Jennifer Ebert agreed to entrust her Private Information to Defendant to receive elective benefits. In exchange, Defendant agreed not only to accept her Private Information, but also to safeguard it and delete it after a reasonable time following the termination of the employment relationship with Jeffrey Ebert. Plaintiff Jennifer Ebert did not reasonably expect that she was providing her Private Information to Defendant forever.

113. Defendant was in possession of Plaintiff Jennifer Ebert's Private

Information before, during, and after the Data Breach.

114. In or around May 2023, Plaintiff Jennifer Ebert received a Notice Letter from Defendant informing her that she was a victim of the Data Breach and that an unauthorized actor “took or viewed certain files” in the Data Breach, which included her Private Information.

115. As a direct and traceable result of the Data Breach, Plaintiff Jennifer Ebert has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes researching the Data Breach, reviewing, and monitoring her accounts for fraudulent activity, reviewing her credit reports, and/or researching credit monitoring services. However, this is not the end. Plaintiff Jennifer Ebert and Class Members will be forced to expend additional time to review their credit reports and monitor their accounts for the rest of their lives. This is time spent at Defendant’s direction, which has been lost forever and cannot be recaptured.

116. Plaintiff Jennifer Ebert places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Jennifer Ebert entrusted her Private Information to Defendant with the understanding that Defendant would keep her information secure and would employ reasonable and adequate security measures to ensure that her Private Information would not be compromised.

117. Plaintiff Jennifer Ebert has never knowingly transmitted unencrypted

Private Information over the internet or any other unsecured source.

118. As a direct and traceable result of the Data Breach, Plaintiff Jennifer Ebert suffered actual damages such as: (1) lost time related to monitoring her accounts and credit reports for fraudulent activity; (2) loss of privacy due to her Private Information being exposed to cybercriminals; (3) loss of the benefit of the bargain because Defendant did not adequately protect her Private Information; (4) exposure to increased and imminent risk of fraud and identity theft now that her Private Information has been exposed; (5) the loss in value of her Private Information due to her Private Information being in the hands of cybercriminals who can use it at their leisure; and (6) other economic and non-economic harm.

119. Plaintiff Jennifer Ebert has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for *years* to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the increased risk of future harm Plaintiffs and the Class now face by offering complimentary credit monitoring services to Plaintiffs and the Class.

120. Plaintiff Jennifer Ebert has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court

intervention, Plaintiffs', and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

121. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

122. Plaintiffs bring this action against PRGX on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the "Class") defined as follows:

All persons residing in the United States whose PHI and/or PII was potentially compromised in the Data Incident.

123. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

124. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

125. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief,

Defendant's own business records or electronic media can be utilized for the notice process.

126. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

127. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has reported that the total number of individuals impacted by the Data Breach was **13,231** individuals.⁶⁷

128. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through PRGX's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of PRGX.

129. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action

⁶⁷ See <https://apps.web.maine.gov/online/aeviewer/ME/40/f674c5b1-aad3-4c7f-84ac-422031509727.shtml>.

vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

130. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. 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 members of the Class individually to effectively redress PRGX'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 benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

131. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;

- b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Private Information;
- c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Private Information, and whether it breached this duty;
- d. Whether PRGX breached its duties to Plaintiffs and the Class as a result of the Data Breach;
- e. Whether PRGX failed to provide adequate cybersecurity;
- f. Whether PRGX knew or should have known that its computer and network security systems were vulnerable to cyberattacks;
- g. Whether PRGX's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;
- h. Whether PRGX was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within its network;
- i. Whether PRGX was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees;
- j. Whether PRGX breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their Private Information;

- k. Whether PRGX failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;
- l. Whether PRGX continues to breach duties to Plaintiffs and the Class;
- m. Whether Plaintiffs and the Class suffered injury as a proximate result of PRGX's negligent actions or failures to act;
- n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and
- o. Whether PRGX's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

- 95. Plaintiffs incorporate paragraphs 1–94 as though fully set forth herein.
- 96. PRGX solicited, gathered, and stored the Private Information of Plaintiffs and Class Members.

97. Upon accepting and storing the Private Information of Plaintiffs and Class members on its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiffs and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

98. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class members could and would suffer if the Private Information was wrongfully disclosed. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

99. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their Private Information, including names, Social Security numbers, and other Private Information.

100. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiffs and Class members in its possession was only used for the provided purpose and that Defendant would destroy any Private Information that it was not required to maintain.

101. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

102. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class members' Private Information from being foreseeably accessed, and its improper retention of Private Information it was not required to maintain, Defendant negligently failed to observe and perform its duty.

103. Plaintiffs and Class members did not receive the benefit of the bargain with Defendant, because providing their Private Information was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

104. Defendant was aware of the fact that cybercriminals routinely target large corporations through cyberattacks in an attempt to steal customer and employee Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

105. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard or delete such data and providing notification

to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

106. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

107. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;
- b. To protect Plaintiffs' and Class members' Private Information in its possession by using reasonable and adequate security procedures and systems;

- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and
- d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

108. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiffs and the Class had entrusted to it.

109. Plaintiffs' injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

110. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class members' Private Information. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the Private Information in its possession;
- b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;
- c. Failing to consistently enforce security policies aimed at protecting Plaintiffs and the Class's Private Information;

- d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- e. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their Private Information.

111. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

112. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

113. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class members while it was within Defendant's possession and control.

114. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and

Class members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

115. Plaintiffs and Class members could have taken actions earlier had they been timely notified of the Data Breach.

116. Plaintiffs and Class members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

117. Plaintiffs and Class members have suffered harm from the delay in notifying them of the Data Breach.

118. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

119. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

120. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

121. Plaintiffs incorporate paragraphs 1–94 as though fully set forth herein.

122. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and the Class.

123. The FTC Act prohibits “unfair practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of Defendant’s duty in this regard.

124. Defendant gathered and stored the Private Information of Plaintiffs and the Class as part of their business, which solicitations and services affect commerce.

125. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

126. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs’ and Class members’ Private Information, and by failing to provide prompt notice without reasonable delay.

127. Defendant’s multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

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

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

130. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Private Information.

131. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

132. Defendant's violations of the FTC Act constitute negligence *per se*.

133. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

134. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

135. Plaintiffs and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

**THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)**

132. Plaintiffs incorporate paragraphs 1–94 as though fully set forth herein.

133. Defendant acquired and maintained the Private Information of Plaintiffs and the Class including their Social Security numbers and other financial information to provide services and/or provide employment.

134. In exchange, Defendant entered into implied contracts with Plaintiffs and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs’ and Class Members’ Private Information and timely notify them of a Data Breach.

135. Based on Defendant’s representations, legal obligations, and acceptance of Plaintiffs’ and the Class Members’ Private Information, Defendant had an implied duty to safeguard their Private Information through the use of reasonable industry standards.

136. Defendant breached the implied contracts by failing to safeguard Plaintiffs’ and Class Members’ Private Information and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took PRGX over an entire year to warn Plaintiffs and Class Member of their imminent risk of identity theft.

137. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' Private Information.

138. Plaintiffs and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

**FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)**

139. Plaintiffs incorporate paragraphs 1–94 as though fully set forth herein.

140. Plaintiffs allege this claim in the alternative to their breach of implied contract claim.

141. Through the use of Plaintiffs' and the Class's Private Information, Defendant received monetary benefits, such as business revenue.

142. Defendant collected, maintained, and stored the Private Information of Plaintiffs and the Class, and as such, Defendant had direct knowledge of the monetary benefits conferred upon it by Plaintiff and the Class.

143. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

144. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

145. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

146. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

147. If Plaintiffs and Class Members knew that Defendant had not secured their Private Information, they would not have allowed Defendant to collect their Private Information.

148. Plaintiffs and Class Members have no adequate remedy at law.

149. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to

prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

150. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

151. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, all gains that they unjustly received.

**FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiffs and the Class)**

152. Plaintiffs incorporate paragraphs 1–94 as though fully set forth herein.

153. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

154. As previously alleged, Plaintiffs and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the Private Information collected from Plaintiffs and the Class.

155. Defendant owed and still owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' Private Information.

156. Upon reason and belief, Defendant still possesses the Private Information of Plaintiffs and the Class members.

157. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

158. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

159. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

160. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their Private

Information and Defendant's failure to address the security failings that led to such exposure.

161. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

162. Plaintiffs and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

- d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;
- f. Ordering that Defendant conduct regular database scanning and security checks; and
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
- e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Second Amended Class Action Complaint.

Dated: July 31, 2024

Respectfully submitted,

/s/: William B. Federman

William B. Federman

(admitted pro hac vice)

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com

James M. Evangelista

Georgia Bar No. 707807

EVANGELISTA WORLEY LLC

500 Sugar Mill Road, Suite 245A
Atlanta, GA 30350
T: 404-205-8400
F: 404-205-8395
E: jim@ewlawllc.com

CERTIFICATE OF SERVICE

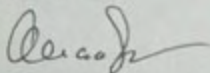
The undersigned hereby certifies that the foregoing was electronically filed with the Clerk of Court using the CM/ECF system, which in turn will automatically serve all counsel of record.

/s/ William B. Federman

Exhibit 1

For More Information. If you have additional questions, you may our call center at 1-888-567-0207 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to PRGX at 200 Galleria Parkway, Suite 450, Atlanta, GA 30339, Attn: Chief Compliance Officer.

Sincerely,



Alicia Jackson
Chief Compliance Officer
PRGX Global, Inc.

Steps You Can Take to Help Protect Minor Child Information

Enroll in Monitoring Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 8, 2023.

2. Telephone. Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring Services

1. **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 2, 2023.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

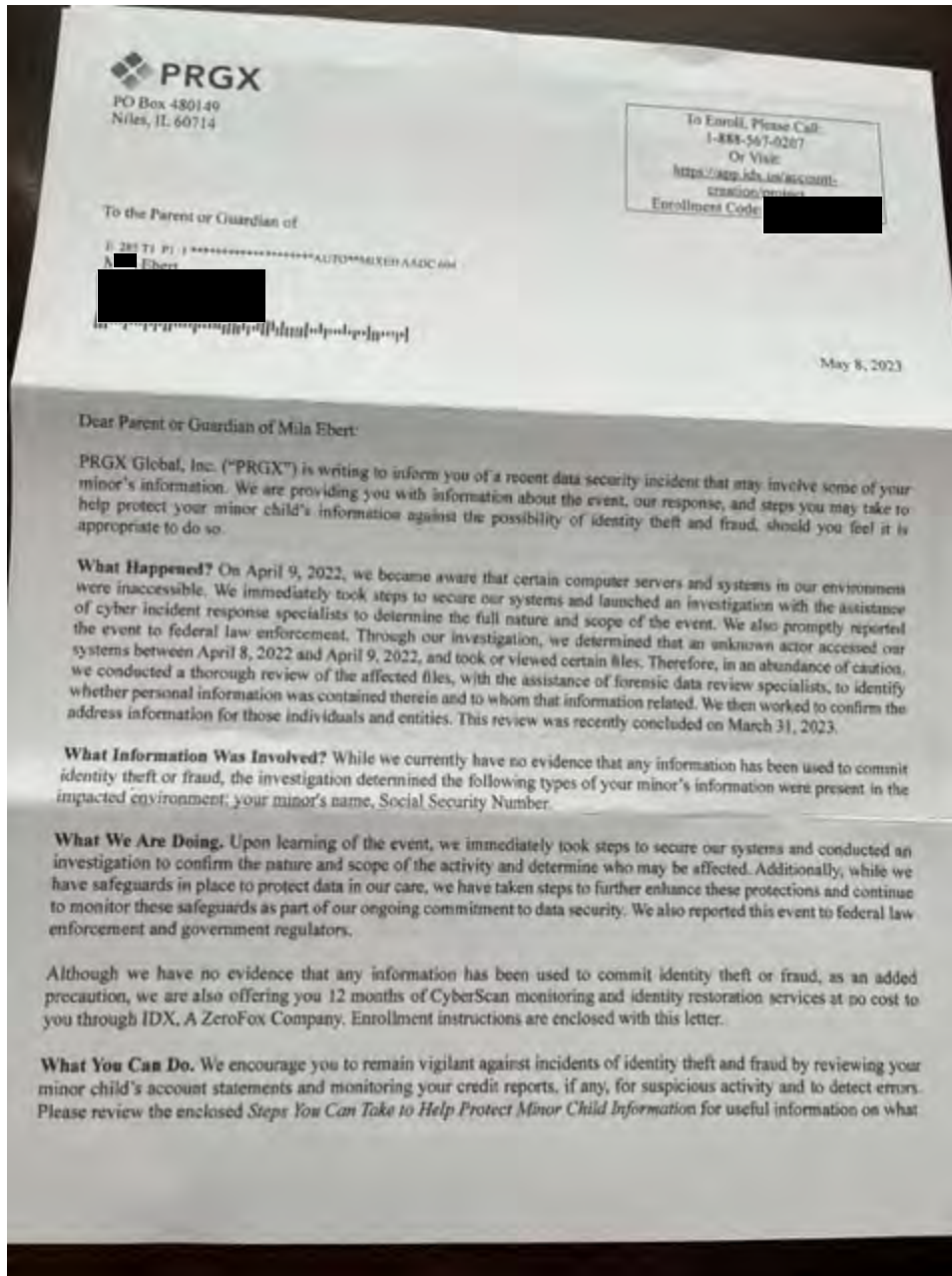
Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

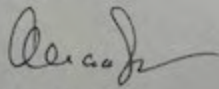
Exhibit 2



you can do to better protect against possible misuse of your minor child's information. You may also enroll your minor in the free minor monitoring services we have provided.

For More Information. If you have additional questions, you may our call center at 1-888-567-0207 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to PRGX at 200 Galleria Parkway, Suite 450, Atlanta, GA 30339, Attn: Chief Compliance Officer.

Sincerely,

A handwritten signature in black ink, appearing to read 'Alicia Jackson', written in a cursive style.

Alicia Jackson
Chief Compliance Officer
PRGX Global, Inc.

Steps You Can Take to Help Protect Minor Child Information

Enroll in Monitoring Services

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 8, 2023.
- 2. Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring Services

1. **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 2, 2023.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

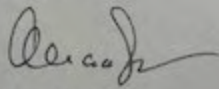
Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Exhibit 3

you can do to better protect against possible misuse of your minor child's information. You may also enroll your minor in the free minor monitoring services we have provided.

For More Information. If you have additional questions, you may our call center at 1-888-567-0207 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to PRGX at 200 Galleria Parkway, Suite 450, Atlanta, GA 30339, Attn: Chief Compliance Officer.

Sincerely,

A handwritten signature in black ink, appearing to read 'Alicia Jackson', written over a light-colored background.

Alicia Jackson
Chief Compliance Officer
PRGX Global, Inc.

Steps You Can Take to Help Protect Minor Child Information

Enroll in Monitoring Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 8, 2023.

2. Telephone. Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring Services

1. **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 2, 2023.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

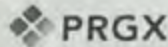
Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Exhibit 4

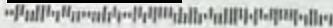


PO Box 480149
Niles, IL 60714

To Enroll, Please Call:
1-888-567-0207
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [REDACTED]

To the Parent or Guardian of

SPENCER EBERT *****AUTO**MIXED**AADC**004
S [REDACTED] Ebert



May 8, 2023

Dear Parent or Guardian of Spencer Ebert:

PRGX Global, Inc. ("PRGX") is writing to inform you of a recent data security incident that may involve some of your minor's information. We are providing you with information about the event, our response, and steps you may take to help protect your minor child's information against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On April 9, 2022, we became aware that certain computer servers and systems in our environment were inaccessible. We immediately took steps to secure our systems and launched an investigation with the assistance of cyber incident response specialists to determine the full nature and scope of the event. We also promptly reported the event to federal law enforcement. Through our investigation, we determined that an unknown actor accessed our systems between April 8, 2022 and April 9, 2022, and took or viewed certain files. Therefore, in an abundance of caution, we conducted a thorough review of the affected files, with the assistance of forensic data review specialists, to identify whether personal information was contained therein and to whom that information related. We then worked to confirm the address information for those individuals and entities. This review was recently concluded on March 31, 2023.

What Information Was Involved? While we currently have no evidence that any information has been used to commit identity theft or fraud, the investigation determined the following types of your minor's information were present in the impacted environment: your minor's name, Social Security Number.

What We Are Doing. Upon learning of the event, we immediately took steps to secure our systems and conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we have taken steps to further enhance these protections and continue to monitor these safeguards as part of our ongoing commitment to data security. We also reported this event to federal law enforcement and government regulators.

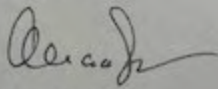
Although we have no evidence that any information has been used to commit identity theft or fraud, as an added precaution, we are also offering you 12 months of CyberScan monitoring and identity restoration services at no cost to you through IDX, A ZeroFox Company. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor child's account statements and monitoring your credit reports, if any, for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Minor Child Information* for useful information on what

you can do to better protect against possible misuse of your minor child's information. You may also enroll your minor in the free minor monitoring services we have provided.

For More Information. If you have additional questions, you may our call center at 1-888-567-0207 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to PRGX at 200 Galleria Parkway, Suite 450, Atlanta, GA 30339, Attn: Chief Compliance Officer.

Sincerely,



Alicia Jackson
Chief Compliance Officer
PRGX Global, Inc.

Steps You Can Take to Help Protect Minor Child Information

Enroll in Monitoring Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 8, 2023.

2. Telephone. Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring Services

1. **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 2, 2023.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Exhibit 5

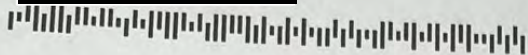


PO Box 480149
Niles, IL 60714

To Enroll, Please Call:
1-888-567-0207
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code [REDACTED]

C 6200 T21 P1 2 *****AUTO**ALL FOR AADC 852

Jennifer Ebert
[REDACTED]



May 8, 2023

Dear Jennifer Ebert:

PRGX Global, Inc. ("PRGX") is writing to inform you of a recent data security incident that may involve some of your information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On April 9, 2022, we became aware that certain computer servers and systems in our environment were inaccessible. We immediately took steps to secure our systems and launched an investigation with the assistance of cyber incident response specialists to determine the full nature and scope of the event. We also promptly reported the event to federal law enforcement. Through our investigation, we determined that an unknown actor accessed our systems between April 8, 2022 and April 9, 2022, and took or viewed certain files. Therefore, in an abundance of caution, we conducted a thorough review of the affected files, with the assistance of forensic data review specialists, to identify whether personal information was contained therein and to whom that information related. We then worked to confirm the address information for those individuals and entities. This review was recently concluded on March 31, 2023.

What Information Was Involved? While we currently have no evidence that any information has been used to commit identity theft or fraud, the investigation determined the following types of your information were present in the impacted environment: your name, Social Security Number.

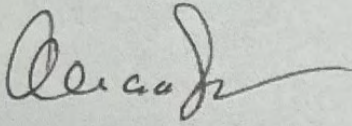
What We Are Doing. Upon learning of the event, we immediately took steps to secure our systems and conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we have taken steps to further enhance these protections and continue to monitor these safeguards as part of our ongoing commitment to data security. We also reported this event to federal law enforcement and government regulators.

Although we have no evidence that any information has been used to commit identity theft or fraud, as an added precaution, we are also offering you 12 months of credit monitoring and identity restoration services at no cost to you through IDX, A ZeroFox Company. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Your Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the free credit monitoring services we have provided for you.

For More Information. If you have additional questions, you may call our call center at 1-888-567-0207 (toll free), Monday through Friday, 9 am to 9 pm Eastern Time, excluding U.S. holidays. You may also write to PRGX at 200 Galleria Parkway, Suite 450, Atlanta, GA 30339, Attn: Chief Compliance Officer.

Sincerely,

A handwritten signature in black ink, appearing to read 'Alicia Jackson', written in a cursive style.

Alicia Jackson
Chief Compliance Officer
PRGX Global, Inc.

Steps You Can Take to Help Protect Minor Child Information

Enroll in Monitoring Services

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 8, 2023.

2. Telephone. Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's identity.

Monitor Your Accounts

To protect against the possibility of identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports for suspicious activity. While minors under the age of 18 typically do not have credit files, the following information relates to protecting one's credit once established.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7 Rhode Island residents that may be impacted by this event.

Steps You Can Take to Help Protect Your Personal Information

Enroll in Credit Monitoring Services

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is August 2, 2023.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-888-567-0207 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below: