IN THE CIRCUIT COURT OF COOK COUNTY, ILLINOIS
COUNTY DEPARTMENT, CHANCERY DIVISION

JUAN GARCIA-MEZA, Individually and on behalf of all others similarly situated, PLAINTIFF, **v.** **CONVERGENT OUTSOURCING, INC.,** DEFENDANT.	Case No.: Hon. Calendar Courtroom

12-Person Jury

CLASS ACTION COMPLAINT

Plaintiff Juan Garcia-Meza, individually and on behalf of all others similarly situated, brings this Class Action Complaint and Demand for Jury Trial against Defendant to seek redress for the defendant's conduct leading up to, surrounding, and following a data vulnerability and breach incident that exposed the personal information of hundreds of thousands of their customers. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including an investigation conducted by his attorneys.

NATURE OF THE CASE

1. Defendant Convergent Outsourcing, Inc. ("Convergent" or "Defendant") failed to safeguard the confidential personal identifying information of Plaintiff Juan-Garcia Meza ("Plaintiff") and hundreds of thousands of individuals ("Class Members" or collectively as the "Class"). This class action is brought on behalf of Class Members whose personally identifiable information ("PII" or "Personal Information") was

stolen by cybercriminals in a cyber-attack that accessed sensitive information through the Defendant's computer system. (the "Data Breach")

2. Defendant's failure to implement or maintain adequate data security measures for personal information directly and proximately caused injuries to Plaintiff and the Classes.

3. Defendant failed to take reasonable steps to employ adequate security measures or to properly protect sensitive Personal Information despite well-publicized data breaches at numerous businesses and financial institutions in recent years.

4. Despite numerous and high-profile data breaches, Defendant failed to implement basic security measures to prevent unauthorized access to this information.

5. Citizens from Illinois and across the United States have suffered real and imminent harm as a direct consequence of Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems, as well as the data stored therein, were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to disclose to its customers the material facts that it did not have adequate computer systems and security practices to safeguard Personal Information; and (d) failing to provide timely and adequate notice of the data breach.

6. The Data Breach was the inevitable result of Defendant's inadequate data security measures and approach to data security. Despite the well-publicized

and ever-growing threat of security breaches, and despite the fact that data breaches were and are occurring across numerous industries, Defendant failed to ensure that it maintained adequate data security measures causing the Personal Information Plaintiff and Class Members to be stolen.

7. As a direct and proximate consequence of Defendant's negligence, a massive amount of customer information was stolen from Defendant. Upon information and belief, Defendant's Data Breach compromised the Personal Information of hundreds-of-thousands (if not more) of Individuals. Victims of the Data Breach have had their Personal Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

8. The Defendant's wrongful actions and/or inaction constitute violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, common law negligence, and invasion of privacy by the public disclosure of private facts.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

10. Plaintiff, on behalf of himself and the Class seeks (i) actual damages, economic damages, emotional distress damages, statutory damages and/or nominal

damages, (ii) punitive damages, (iii) injunctive relief, and (iv) fees and costs of litigation.

JURISDICTION AND VENUE

11. Jurisdiction over the Defendant is proper under 735 ILCS 5/2-209(a)(l) (transaction of any business within this State), section 2-209(b)(4) (corporation doing business within this State), and section 2-209(c) (any other basis now or hereafter permitted by the Illinois Constitution and the Constitution of the United States).

12. Venue is proper in this county pursuant to 735 ILCS 5/2-101, because this is the county in which the transactions and occurrences at issue, or some part thereof, occurred. In addition, Defendant regularly does business in this county. 735 ILCS 5/2-102(a).

13. Pursuant to General Order No. 1.2 of the Circuit Court of Cook County, this action is properly before the Chancery Division of the County Department because it is a putative Class Action.

PARTIES

14. Plaintiff Juan Garcia-Meza was a resident and citizen of the State of Illinois during all times relevant to this complaint.

15. Defendant Convergent Outsourcing, Inc. is a Washington based corporation with its primary place of business located at 800 SW 39th St, Suite 100, Renton, Washington 98057.

FACTUAL ALLEGATIONS

A. The Data Breach

16. Defendant is a debt collector that operates nationally and as a result has significant amounts of information on consumers that it seeks to collect debts from.

17. On or about June 17, 2022, Defendant became aware of a data breach that occurred on its computer systems.

18. Defendant later determined that the information accessed by the cybercriminals contained personal information belonging to the Class Members.

19. In October 2022 Defendant notified many of its customers that an unauthorized person, or persons, had access to Defendant's accounts on its computer systems, compromising information it held on many of its customers, including data submitted by creditors who used Defendant to collect debts from consumer or otherwise service accounts.

20. Defendant waited months after it allegedly became aware of the Data Breach before it notified consumers that it had lost their Personal Information.

21. The cybercriminals accessed insufficiently protected information belonging to Plaintiff and the Class Members. Upon information and belief, as a result of Defendant's failure to properly secure Plaintiff's and the Class Members' personal information, the cybercriminals obtained extensive personal information including but not necessarily limited to:

A. Names;

B. Contact information;

C. Financial account information, and

D. Social security numbers.

22. Plaintiff's and Class Members' sensitive personal information, which was entrusted to Defendant, its officials and agents, was compromised, unlawfully accessed, and stolen due to the data breach.

23. As a result of Defendant's actions and/or inaction, Plaintiff and the Class Members were harmed and must now take remedial steps to protect themselves from future loss. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse of their Personal Information in the coming months and years, including but not limited to unauthorized account access including on third-party services and identity theft through use of personal information to open up accounts.

24. In late October 2022, months since the breach occurred, Defendant began notifying consumers of the Data Breach.

25. Defendant indicated that it had lost information related to its debt collection accounts as well as other information it held on consumers who had their accounts referred to Defendant for collection or servicing.

26. On information and belief, even though hundreds of thousands of consumers have had their personal data breached due to Defendant's actions and inactions, the Defendant has not specifically provided notice to all of these consumers.

27. The criminals were able to access Plaintiff's and the Class's personal information because Defendant failed to take reasonable measures to protect the Personally Identifiable Information they collected and stored. Among other things,

Defendant failed to implement data security measures designed to prevent this attack, despite repeated industry wide warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

28. As a result of Defendant's failure to properly secure Plaintiff's and the Class Members' personal identifying information, Plaintiff's and the Class Members' privacy has been invaded.

29. Moreover, all of this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have likely accessed and viewed Plaintiff's and the Class Members' PII.

E. Data Breaches and Industry Standards of Protection of PII

30. Identity theft, which costs Americans billions of dollars a year, occurs when an individual's personal identifying information is used without his or her permission to commit fraud or other crimes. Victims of identity theft typically lose hundreds of hours dealing with the crime, and they typically lose hundreds of dollars.

31. According to the Federal Trade Commission ("FTC"):

> **Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.**

32. The United States Government Accountability Office ("GAO") has stated that identity thieves can use identifying data to open financial accounts and incur

charges and credit in a person's name. As the GAO has stated, this type of identity theft is the most damaging because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim's credit rating. Like the FTC, the GAO explained that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

33. Industry Standards highlight several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

34. Identity theft crimes often encompass more than just immediate financial loss. Identity thieves often hold onto stolen personal and financial information for several years before using and/or selling the information to other identity thieves.

35. Accordingly, federal and state legislatures have passed laws to ensure companies protect the security of sensitive personally identifying confidential information, such as that wrongfully disclosed in the Data Breach.

36. The FTC has issued a publication entitled "Protecting Personal Information: A Guide for Business" ("FTC Report"). The FTC Report provides guidelines for businesses on how to develop a "sound data security plan" to protect

against crimes of identity theft. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow, among other things, the following guidelines:

a. Know what personal information you have in your files and on your computers;

b. Keep only what you need for your business;

c. Protect the information that you keep;

d. Properly dispose of what you no longer need;

e. Control access to sensitive information by requiring that employees use "strong" passwords; tech security experts believe the longer the password, the better; and

f. Implement information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information.

37. The FTC Report also instructs companies that outsource any business functions to proactively investigate the data security practices of the outsourced company and examine their standards.

38. The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

39. Upon information and belief, the Defendant has policies and procedures in place regarding the safeguarding of confidential information they are entrusted with, and Defendant failed to comply with those policies. Defendant also negligently failed to comply with industry standards or even implement rudimentary security practices, resulting in Plaintiff's and the Class's confidential information being substantially less safe than had this information been entrusted with other similar companies.

40. Defendant was aware of the likelihood and repercussions of cyber security threats, including data breaches, having doubtlessly observed numerous other well-publicized data breaches involving major corporations over the last decade- as well as the numerous other similar data breaches preceding those major breaches.

41. In addition to Defendant's failure to prevent the Data Breach, Defendant also failed to detect the Data Breach and realize this Personal Information remained publicly accessible and unencrypted for a substantial amount of time.

42. Hackers, cyber-criminals, and other nefarious actors, therefore, had sufficient time to collect this Personal Information unabated. During this time, Defendant failed to recognize the failure to protect this Personal Information. If Defendant had quickly detected the Data Breach, this likely would have significantly reduced the consequences of the Data Breach. Instead, Defendant's delay in detecting the Data Breach contributed to the scale of the Data Breach and the resulting damages.

43. The Data Breach occurred because Defendant failed to implement adequate data security measures to protect its database and computer systems from the potential dangers of a data breach and failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach.

44. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting Personal Information.

F. Defendant's Data Breach caused Current and Future Harm

45. As a direct and proximate result of Defendant's wrongful disclosure, criminals now have Plaintiff's and the Class Members' Personal Information. Additionally, the disclosure of their Personal Information makes Plaintiff and Class Members much more likely to respond to requests from Defendant or law enforcement agencies for more personal information, such as bank account numbers, login information or other highly personal PII. Because criminals know this and are capable of posing as Defendant or law enforcement agencies, consumers like Plaintiff and fellow Class Members are more likely to unknowingly give away their sensitive personal information to other criminals.

46. Defendant's wrongful actions and inactions here directly and proximately caused the public disclosure of Plaintiff's and Class Members' personal identifying information without their knowledge, authorization and/or consent. As a further direct and proximate result of Defendant's wrongful actions and/or inaction,

Plaintiff and Class Members have suffered, and will continue to suffer, damages including, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

47. As a further result of the data breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

48. Identity thieves can use personal information, such as that of Plaintiff, the other Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. Even basic personal information, combined with other contact information, is very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if some information was not involved in the Data breach, the unauthorized parties could use Plaintiff's and Class Members' Personal Information to access other information, including, but not limited to email accounts, government services accounts, e-commerce accounts, payment card information, and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

49. Defendant was at all times fully aware of its obligations to protect the Personal Information of Plaintiff and Class Members. While Plaintiff and Class Members did not specifically choose Defendant to attempt to collect debts from them or otherwise service their financial accounts, they would have taken additional

precautions if they knew the Defendant would fail to maintain adequate data security. Defendant was also aware of the significant repercussions that would result from their failure to do so.

50. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Identity theft victims must spend numerous hours and their own money repairing the impact to their credit.

51. Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class Members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges, identity theft, or other financial loss as a result of the Data Breach.

52. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff, the other Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Theft of their Personal Information and financial information;

b. Costs for credit monitoring services; unauthorized charges on their debit and credit card accounts;

c. Unauthorized charges on their debit and credit cards;

d. Injury flowing from potential fraud and identity theft posed by their credit/debit card and Personal Information being placed in the

hands of criminals and already misused via the sale of Plaintiff and Class members' Personal Information on the black market and dark web;

e. Losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

f. Losses in the form of deprivation of the value of their Personal Information;

g. The untimely and inadequate notification of the Data Breach;

h. The improper disclosure of their Customer Data;

i. Loss of privacy;

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

k. The loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services.

53. Additionally, even with credit monitoring, the damages of a Data Breach will last much longer since this Personal Information cannot be completely removed from the possession of cybercriminals. In fact, it will likely continue to circulate on the dark web and be sold or traded to other hackers and cybercriminals or identity thieves who will use it to continue to perpetuate fraud against the Class Members.

54. Although the Personal Information of Plaintiff and the Class Members has been stolen, Defendant continues to hold Personal Information of the affected individuals, including Plaintiff and the Class Members.

55. Particularly, because Defendant has demonstrated an inability to prevent a data breach or stop it from continuing even after being detected and informed of the impermissible dissemination—Plaintiff, the other Class members, have an undeniable interest in ensuring their Personal Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further disclosure and theft.

56. Accordingly, Plaintiff on behalf of himself and the Class, brings this action against Defendant seeking redress for their unlawful conduct.

CLASS ALLEGATIONS

57. Plaintiff brings these claims on behalf of the following classes:

National Class: All individuals whose PII was exposed while in the possession of Defendant, or any of its subsidiaries and/or agents, during the Data Breach.

Illinois Sub-Class: All individuals in Illinois whose PII was exposed while in the possession of Defendant, or any of its subsidiaries and/or agents, during the Data Breach.

58. Plaintiff may alter the class definitions to conform to developments in the case and discovery.

59. The proposed classes meet all requirements under 735 ILCS 5/2-801.

60. The putative Classes are comprised of thousands of persons, making joinder impracticable. The joinder of the Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the Court. The Classes can be identified through the Defendant's records or the Defendant's agents' records.

61. The rights of each Class Member were violated in an identical manner as a result of Defendant's willful, reckless and/or negligent actions and/or inaction.

62. **Numerosity:** Upon information and belief, the Classes are so numerous that joinder of all individual plaintiffs would be impracticable. The exact number of members of the Classes are presently unknown and can only be ascertained through discovery because that information is exclusively in the possession of Defendant. However, it is reasonable to infer that more than 40 individuals in each class were impacted by the data breach at issue. Members of the Classes can be easily identified through Defendant's records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

63. **Commonality and Predominance:** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Classes, including, without limitation:

a. Whether Defendant negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class Members' personal identifying information;

b. Whether Defendant was negligent in storing and failing to adequately safeguard Plaintiff's and Class Members' personal identifying information;

c. Whether Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in protecting and securing their personal identifying information;

d. Whether Defendant breached its duties to exercise reasonable care in failing to protect and secure Plaintiff's and Class Members' personal identifying information;

e. Whether by disclosing Plaintiff's and Class Members' personal identifying information without authorization, Defendant invaded Plaintiff's and Class Members' privacy;

f. Whether Plaintiff and Class Members sustained damages as a result of Defendant's failure to secure and protect their personal identifying information.

64. **Adequacy of Representation:** Plaintiff is an adequate representative of the Classes because his interests do not conflict with the interests of the members of the Classes he seeks to represent, and he intends to prosecute this action vigorously. Plaintiff has retained counsel competent and experienced in consumer class actions and complex litigation. The interests of the Class will be

fairly and adequately protected by Plaintiff and his counsel and Plaintiff's claims are typical of the claims of the class members.

65. **Appropriateness:** A class action in this case would be appropriate and superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Classes are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Classes to individually seek redress for Defendant's wrongful conduct. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the judicial system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

66. Defendant has acted or failed to act on grounds that apply generally to the class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/1, *ET SEQ.* (ON BEHALF OF PLAINTIFF AND THE ILLINOIS SUBCLASS)

67. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

68. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

> **Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.**

69. Defendant violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff.

70. Specifically, it was an unfair act and practice to represent to Plaintiff and the Illinois Subclass members that it implemented commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations, including by failing to timely detect the Data Breach.

71. Despite representing to Plaintiff and the Illinois Subclass members that it would implement commercially reasonable measures to protect their PII, Defendant nonetheless failed to fulfill such representations.

72. Plaintiff and the Illinois Subclass members have suffered injury in fact and actual damages, as alleged herein, as a result of Defendant's unlawful conduct and violations of the ICFA and analogous state statutes.

73. Defendant's conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers PII.

74. An award of punitive damages is appropriate because Defendant's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of the Plaintiff and consumers, generally, and Plaintiff had no choice but to submit to Defendant's illegal conduct.

COUNT II - NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE CLASS)

75. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

76. Upon Defendant accepting and storing the Personal Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Personal Information was private and confidential and should be protected as private and confidential.

77. Defendant owed a duty of care not to subject Plaintiff's and the Class's Personal Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

78. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' personal identifying information would result in an unauthorized third-party gaining access to such information for no lawful purpose, and that such third parties would

use Plaintiff's and Class Members' personal identifying information for malevolent and unlawful purposes, including the commission of direct theft and identity theft.

79. Defendant knew, or should have known, of the risks inherent in collecting, storing, and sharing Personal Information amongst themselves and the importance of adequate security. Defendant knew of should have known about numerous well-publicized data breaches within the industry.

80. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's failure to secure and protect their personal identifying information as a result of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft herein, insurance incurred in mitigation, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they suffered loss and are entitled to compensation.

81. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, negligence at common law.

COUNT III - INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS AND INTRUSION UPON SECLUSION (ON BEHALF OF PLAINTIFF AND THE CLASS)

82. Plaintiff re-alleges the preceding paragraphs as is set forth fully in this Count.

83. Plaintiff's and Class Members' Personal Identifying Information is and always has been private.

84. Dissemination of Plaintiff's and Class Members' Personal Information is not of a legitimate public concern; publication to third parties of their personal identifying information would be, is and will continue to be, offensive to Plaintiff, Class Members, and other reasonable people.

85. Plaintiff and the Class Members were (and continue to be) damaged as a direct and proximate result of Defendant's invasion of their privacy by publicly disclosing their private facts including, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, for which they are entitled to compensation.

86. Defendant's wrongful actions and/or inaction (as described above) constituted, and continue to constitute, an invasion of Plaintiff's and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their personal identifying information).

REQUEST FOR RELIEF

WHEREFORE, Plaintiff asks for an award in his favor and against Defendant as follows:

A. Certifying this action as a class action, with a class as defined above;

B. Designation of Plaintiff as representative of the proposed Class and designation of Plaintiff's counsel as Class counsel;

C. For equitable relief enjoining Defendant from engaging in the wrongful acts and omissions complained of herein pertaining to the misuse and/or disclosure

of Plaintiff's and Class Members' Personal Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

D. Awarding compensatory damages to redress the harm caused to Plaintiff and Class Members in the form of, *inter alia*, direct theft, identity theft, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm. Plaintiff and Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and Class Members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of this Court.

E. Ordering injunctive relief including, without limitation, (i) adequate credit monitoring, (ii) adequate identity theft insurance, (iii) instituting security protocols in compliance with the appropriate standards and (iv) requiring Defendant to submit to periodic compliance audits by a third party regarding the security of personal identifying information in its possession, custody and control.

F. Awarding Plaintiff and the Class Members interest, costs and attorneys' fees;

G. Compensatory damages, punitive damages and attorneys' fees and the costs of this action as allowed under the Illinois Consumer Fraud Act; and

H. Awarding Plaintiff and the Class such other and further relief as this Court deems just and proper.

Respectfully Submitted,

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys

Bryan Paul Thompson
Robert W. Harrer
CHICAGO CONSUMER LAW CENTER, P.C.
Cook County Firm No. 62709
33 N. Dearborn St., Suite 400
Chicago, Illinois 60602
Tel. 312-858-3239
Fax 312-610-5646
bryan.thompson@cclc-law.com
rob.harrer@cclc-law.com

Michael Kind, Esq. (*Pro Hac Vice* Forthcoming)
Nevada Bar No. 13903
KIND LAW
8860 South Maryland Parkway, Suite 106
Las Vegas, NV 89123
Phone: (702 337-2322
FAX: (702) 329-5881
Email: mk@kindlaw.com

DOCUMENT PRESERVATION DEMAND

Plaintiff hereby demands that defendant take affirmative steps to preserve all recordings, data, documents, and all other tangible things that relate to plaintiff, the events described herein, any third party associated with any telephone call, campaign, account, sale or file associated with plaintiff, and any account or number or symbol relating to them. These materials are likely very relevant to the litigation of this claim. If defendant is aware of any third party that has possession, custody, or control of any such materials, plaintiff demands that defendant request that such third party also take steps to preserve the materials. This demand shall not narrow the scope of any independent document preservation duties of the defendant.

By: /s/ *Bryan Paul Thompson*
One of Plaintiff's Attorneys

ClassAction.org