IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

JEFFREY HOVELL, individually and on behalf of all others similarly situated, Plaintiff, v. TERMINIX GLOBAL HOLDINGS, INC., Defendant.	**CASE NO. 2:20-cv-2804** **CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **JURY DEMAND**

CLASS ACTION COMPLAINT

1. Plaintiff, Jeffrey Hovell, individually and on behalf of all others similarly situated, brings this action against Defendant TERMINIX GLOBAL HOLDINGS, INC. ("Terminix" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is in the hundreds of thousands, many of whom have different citizenship from Defendant, including the named Plaintiff here.

3. This Court has jurisdiction over Defendant because it operates and/or is incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

4. Through its business operations in this District, Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Defendant is based in this District, maintains Class Members' personally identifiable information ("PII") in the District and has caused harm to Class Members residing in this District.

NATURE OF THE ACTION

6. This class action arises out of the recent data breach that was allowed by Defendant Terminix, which held in its possession the PII of Defendant's employees, former employees, employees and former employees of Defendant's former affiliate company ServiceMaster, and other personnel across the United States (the "Data Breach").

7. The PII exposed in the Data Breach included, among other things: names, Social Security numbers, dates of birth, employment dates, 401K balances and the name of the relevant 401K provider.

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect the PII of employees, former employees, ServiceMaster employees and former employees, and other personnel.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained.

10. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. Defendant disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard PII; and failing to take standard and reasonably available steps to prevent the Data Breach.

12. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the PII. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

13. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII that Defendant collected and maintained is now in the hands of data thieves.

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits,

filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent 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.

16. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

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

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

19. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract, and (iv) unjust enrichment.

STATEMENT OF FACTS

A. The Data Breach

20. Data breaches can occur in myriad ways. Phishing, a common tool deployed to carry out a data breach, is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted

entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

21. On September 16, 2020, Terminix discovered that one of its employees responded to a phishing scam, which allowed hackers to gain access to the employee's Microsoft Office 365 account. Once inside the employee's Microsoft Office 365 account, the hackers caused the employee's emails to be auto-forwarded from the employee's inbox to an external email account controlled by the hackers.

22. The auto-forwarding began on September 10, 2020 and continued unabated for nearly two weeks until September 22, 2020.

23. Terminix learned that the emails forwarded from the compromised email account contained highly sensitive financial documents of certain employees, former employees and other personnel.

24. The data consisted of a treasure trove of Terminix employees', former employees' and personnel's PII such as names, Social Security numbers, dates of birth, employment dates, 401K balances and the name of the relevant 401K provider.

25. On or about October 9, 2020, Terminix notified affected persons of the Data Breach. The Notice of Data Incident ("Notice") stated in relevant part the following:

Notice of Data Incident

What Happened

On September 16th, the company discovered that a teammate had responded to a phishing scam, which allowed hackers to gain access to the teammate's Office 365 account and cause the teammate's emails to be auto-forwarded from the teammate's inbox to an external email account controlled by the hackers. The auto-forwarding began on September 10th and continued until September 22nd. Please note that this breach involved a hack into Office 365 at the cloud level and there was no malware or malicious software that infected the company's internal systems.

What Information Was Involved
Our review of compromised emails revealed that one email included a file which contained the name, social security number, date of birth, employment dates, 401K balance and the name of our 401K provider for 14,708 current and former teammates across the United States. Due to the sensitive nature of this information, it is possible that thieves can use it for identity theft. We do not know if the information has been used at this time. We are sending this notice to both Terminix and ServiceMaster teammates because these events took place before the completion of the sale of ServiceMaster brands, when everyone receiving this notice was employed under the ServiceMaster Global Holdings brand.

What We Are Doing
We have taken and continue to take a number of actions in response to the breach. We have disabled the forwarding of the emails and contained the breach. We modified our email filtering and account authorization protocol to help prevent similar data breach incidents. We are communicating to our teammates to be sure everyone is especially diligent regarding any potential scams as we continue to fight the battle with these criminals from repeated phishing attacks. We are requiring teammates to complete the annual security awareness training, and we have issued specialized training to particularly high-risk groups to help them recognize extremely sophisticated phishing attempts. We are working with law enforcement agencies to investigate this cybercrime and are notifying state authorities as well. We've notified the provider of our 401K plans and the major credit agencies. We are continuing to monitor the security of our systems and reinforce messages related to the importance of abiding by proper security and data handling measures.

What You Can Do
While we currently have no reason to believe any personal information has been misused, for your protection, we have arranged to provide identity theft protection services through ID Experts®, the data breach and recovery services expert at no cost to you for two years. MyIDCare services include two years of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

B. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.

26. Terminix acquires, collects, and stores a massive amount of personally identifiable information ("PII") on its employees, former employees and other personnel.

27. As a condition of employment, or as a condition of receiving certain benefits, Terminix requires that employees, former employees and other personnel entrust it with highly sensitive personal information.

28. By obtaining, collecting, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

30. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

C. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

31. Defendant was well-aware that the PII it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes.

32. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[1] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

33. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[1] Federal Trade Commission, *Warning Signs of Identity Theft,* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

34. As one expert explained: "And the problem is this. When your password gets compromised after a data breach, you can change your password. Of course it can be a pain and a nuisance to change your password, but it's not an insurmountable problem – and if you haven't made the mistake of reusing the same password in multiple places the impact of the breach is limited. ***But just try changing the details contained on your passport, your date of birth, your bank account details, or your social security number…***."[2]

35. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on employees, former employees and other personnel as a result of a breach.

36. Defendant knew, or reasonably should have known, of the foreseeable risks associated with data breaches, because data breaches have become so widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.

37. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.[3]

---

[2] https://www.tripwire.com/state-of-security/featured/ge-data-breach-third-party/
[3] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-oftargeted-ransomware?nlpk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utmsource=newsletter&utmmedium=email&utm_campaign=consumerprotection (last visited October 27, 2020)

38. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

39. Phishing attacks of the type that the unauthorized persons used to gain access to Defendant's employee email accounts are among the oldest, most common, and well-known form of cyberattacks. "Phishing is a cyberattack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need—a request from their bank, for instance, or a note from someone in their company—and to click a link or download an attachment."[4] The fake link will typically mimic a familiar website and require the input of credentials. Once inputted, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyber-attacks, dating back to the 1990s" and one that every organization with an internet presence is aware."[5] It remains the "simplest kind of cyberattack and, at the same time, the most dangerous and effective."[6]

40. Phishing attacks are generally preventable with the implementation of a variety of proactive measures such as purchasing and using some sort of commonly available anti-malware security software (such as the ubiquitous Malwarebites). Most cybersecurity tools have the ability to detect when a link or an attachment isn't what it seems.[7] Other proactive measures include sandboxing inbound e-mail (*i.e.* an automated process that segregates e-mail with attachments and links to an isolated test environment, or a "sandbox," wherein a suspicious file or URL may be executed safely), inspecting and analyzing web traffic, penetration testing (which can be used to test an organization's security policy, its adherence to compliance requirements, its employees'

---

[4] Frulingher, J., "What is phishing? How this cyber-attack works and how to prevent it," CSO Online, Apr. 7, 2020, https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html (last visited June 20, 2020).
[5] *Id.*
[6] Phishing, Malwarebytes, https://www.malwarebytes.com/phishing/ (last visited June 20, 2020).
[7] *Id.*

security awareness, and the organization's ability to identify and respond to security incidents), and employee education, just to name some of the well-known tools and techniques to prevent phishing attacks.

41. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the computer systems and data that held the stolen PII. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor the data security systems for existing intrusions, and;

d. Failing to ensure that its agents and service providers with access to Plaintiff's and Class Members' PII employed reasonable security procedures.

D. Defendant Failed to Comply with FTC Guidelines

42. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[8]

[8] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

43. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[9] The guidelines note that businesses should protect the personal customer 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 to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

44. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[10]

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

---

[9] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[10] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

46. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

47. Defendant was at all times fully aware of its obligation to protect the PII of consumers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Fails to Comply with Industry Standards

48. Companies such as Terminix have been identified as being particularly vulnerable to cyber-attacks because of the value of the PII that they maintain. Cybersecurity firms have promulgated a series of best practices that a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[11]

49. The Data Breach appears to be or was caused by a standard credential phishing attack or due to credential reuse on another site.

50. Cybersecurity experts have explicitly noted that phishing attacks can be prevented with adequate staff security training.[12]

[11] https://insights.datamark.net/addressing-bpo-information-security/
[12] https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks.

F. Plaintiff and Class Members Suffered Damages

51. The ramifications of Defendant's failure to keep class members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Individual victims of data breaches are more likely to become victims of identity fraud.

52. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

53. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

54. Defendant is a multi-billion-dollar company and has the resources necessary to prevent the Data Breach, but neglected to adequately invest in data security measures, despite its obligation to protect consumer data.

55. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the theft of PII.

56. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing

increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[13]

57. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[14]

58. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[15]

59. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in

[13] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf

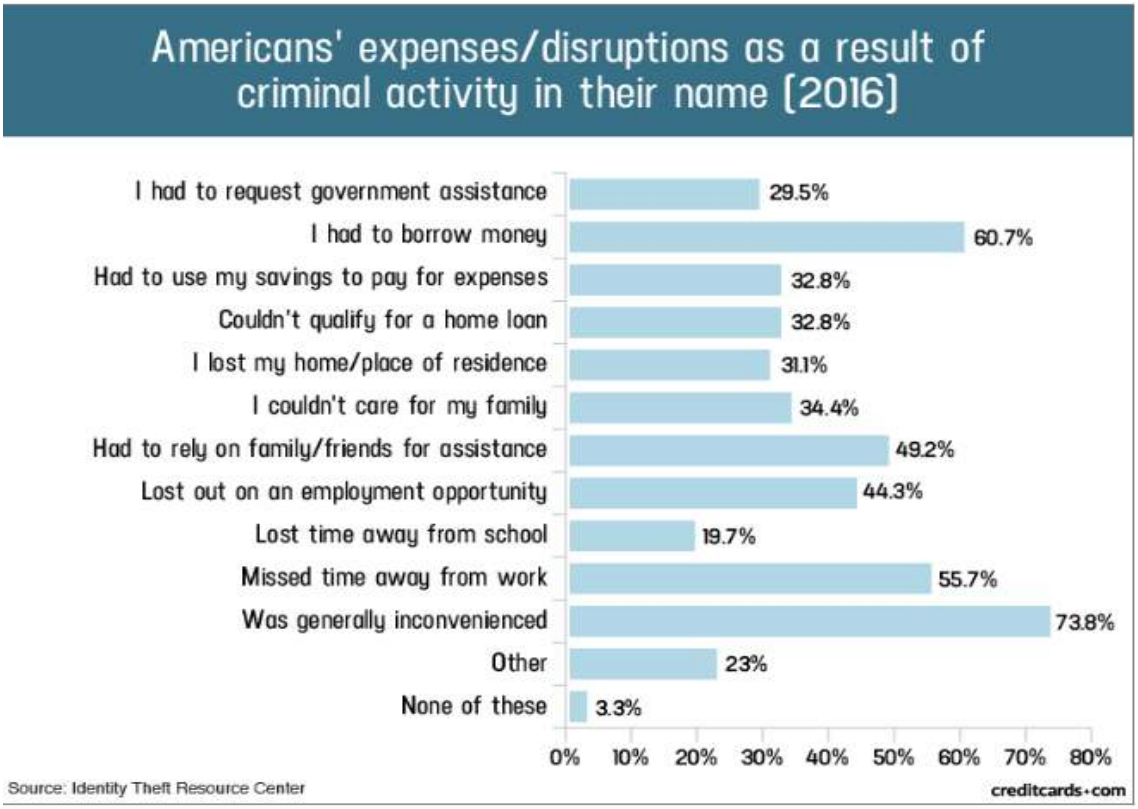
[14] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[15] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

61. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[16]

[16] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



62. What's more, PII constitutes a valuable property right, the theft of which is gravely serious.[17] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

63. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

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

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

64. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

65. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

66. To date, Defendant has merely offered identity theft protection services at no charge for 24 months. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

67. Furthermore, Defendant's offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in identity theft protection services upon discovery of the breach, Defendant merely sent instructions offering the services to affected employees, former employees, and other personnel with the recommendation that they sign up for the services.

68. Even worse, the offer provides a very limited time within which to enroll by setting a deadline of January 11, 2021.

69. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

70. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

71. Indeed, after the Data Breach occurred, Plaintiff Hovell received scam emails, phone calls and text messages, which appeared to be placed with the intent to obtain personal information to commit identity theft by way of a social engineering attack. As a result, Plaintiff Hovell was required to spend time obtaining a credit report and monitoring his credit history and financial accounts for suspicious activity.

72. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

73. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

74. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

75. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

76. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

77. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

78. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

79. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable 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 relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

80. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

81. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains intimate details about a person's life —may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

82. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

PARTIES

83. Plaintiff Jeffrey Hovell is, and at all times mentioned herein was, an individual citizen of the State of Florida. Plaintiff Hovell is a former employee of Terminix. During Plaintiff Hovell's employment at Terminix, he was required to provide his PII to Defendant. On or about

October 20, 2020, Terminix notified Plaintiff Hovell that his PII was stolen and compromised in the Data Breach.

84. Defendant Terminix is a company that offers pest control products and services with its principal place of business at 150 Peabody Place Memphis, TN 38103 United States.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

86. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose PII was compromised as a result of the Data Breach announced by Terminix on or about October 20, 2020 (the "Class").

87. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

88. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

89. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The Class consists of at least 14,000 of employees, former employees, and personnel of Defendant whose data was compromised in the Data Breach.

90. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was *per se* negligent;

l. Whether Defendant was unjustly enriched;

m. Whether Defendant breached an implied contract with Plaintiff and Class Members, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

91. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

92. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

93. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

94. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

95. Defendant has acted 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.

96. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

97. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant Terminix.

CAUSES OF ACTION
FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

98. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 97 above as if fully set forth herein.

99. Defendant required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

100. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information.

101. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

102. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

104. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. §§ 47-18-2105 to 2107 (2005).

105. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. § 47-18-2110 (2018).

106. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members pursuant to Tenn. Code. § 39-14-150(G).

107. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential PII.

108. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII; and

e. Failing to detect in a timely manner that Class Members' PII had been compromised.

109. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was

reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

110. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

111. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

112. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

113. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach

114. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

115. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 97 above as if fully set forth herein.

116. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their use of Defendant's services.

117. Plaintiff and Class Members provided their labor to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure.

118. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

119. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

120. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

121. When Plaintiff and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

122. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

123. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

124. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

125. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

126. Defendant breached their implied contracts with Class Members by failing to safeguard and protect their PII.

127. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

128. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

129. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

130. Plaintiff restates and realleges paragraphs 1 through 97 above as if fully set forth herein.

131. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their labor, and Defendant.

132. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members, and accepted that monetary benefit.

133. 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 themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal 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 Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff 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.

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

135. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

136. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

137. Plaintiff and Class Members have no adequate remedy at law.

138. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (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 PII, 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 PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

140. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

FOURTH COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

141. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 97 above as if fully set forth herein.

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

143. Section 5 of 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 PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

144. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect employee PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

145. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

146. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

147. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

148. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

149. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

150. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they were failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

151. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: November 6, 2020

Respectfully submitted,

John Spragens, TN BPR No. 31445
SPRAGENS LAW PLC
311 22nd Ave. N.
Nashville, TN 37203
T: (615) 983-8900
F: (615) 682-8533
john@spragenslaw.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (202) 429-2290
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class