IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

KENNETH HERETICK, a Florida resident,	**Case No.**
Plaintiff,	**CLASS ACTION COMPLAINT**
v.	**JURY TRIAL DEMANDED**
EXACTIS, LLC, a Florida limited liability company,	
Defendant.	

Plaintiff, KENNETH HERETICK (hereinafter, "Plaintiff"), individually and on behalf of all others similarly situated (the "Class" and "Subclass," as more fully defined below), brings this action against EXACTIS, LLC ("Exactis" or "Defendant"), to recover monetary damages, injunctive relief, and other remedies for violations of federal and state statutes, and common law.

I. INTRODUCTION

1. This case concerns one of the biggest and most damaging data breach cases, exceeding Equifax and other massive data breaches—in both scale and information disseminated.

2. Exactis is a leading compiler and aggregator of premium business and consumer data, boasting over 3.5 billion records of businesses and consumers alike. These records contain people's phone numbers, home and email addresses, personal interests and preferences, ages and genders of their children, and other extremely detailed, personal information—exceeding as many as 400 data points on each business and consumer.

3. As has been revealed in recent high profile data breaches, hackers and other nefarious actors use this information to engage in social engineering and other tactics to gain access to financial and other valuable accounts; financial institutions and other organizations

routinely verify a user's identity with these details to reset passwords, change mailing addresses, and otherwise permit someone to access and change details of their accounts.

4. In collecting, maintaining, and selling this information, Exactis understood it had an enormous responsibility to protect the data it collected, and bragged that its data warehouses are among the biggest and most respected in the digital and direct marketing industry. Except Exactis failed to employ even the most basic forms of security, and left this highly sensitive information of some 230 million consumers and 110 million businesses on a public server—bare, unprotected, and available to anyone to download. Even worse, Exactis did not employ any form of encryption to protect this data.

5. Security researcher Vinny Troia, of Night Lion Security, found this expansive database and proclaimed it contained information on "pretty much every U.S. citizen," and described the database as "one of the most comprehensive collections" of data on individuals and businesses.[1]

6. Despite numerous high-profile data breaches at companies such as Home Depot, Target, and Neiman Marcus, last year's high-profile hack of credit bureau Equifax that exposed the personal data of hundreds of millions of Americans, and the ever-evolving hack of Facebook's user data and information, Defendant failed to implement basic security measures such as a firewall, encryption, and other standard data management practices to prevent unauthorized access to this information.[2]

7. Defendant boasts on its website that "Data is the fuel that powers Exactis. Warehousing over 3.5 billion consumer, business, and digital records, The Exactis Data Cloud

[1] Mike Murphy, *A new data breach may have exposed personal information of almost every American adult*, Market Watch (June 27, 2018) https://www.marketwatch.com/story/a-new-data-breach-may-have-exposed-personal-information-of-almost-every-american-adult-2018-06-27.

[2] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, Wired (June 27, 2018) https://www.wired.com/story/exactis-database-leak-340-million-records/

provides knowledge and insight to hundreds of firms enabling them to achieve marketing success through the use of high quality data. The Exactis data cloud is one of the largest and most respected in the data marketing industry. It is constructed of hundreds of compiled and proprietary data sources, has over 400 different selects, and utilizes a triple verification process to guarantee accurate targeting. This includes demographic, geographic, firmographic, lifestyle, interests, CPG, automotive, and behavioral data."[3]

8. Citizens from 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.

9. As a result of the data breach, personal information of over 230 million people has been exposed to criminals for misuse. Remarkably, Defendant would not have even discovered the breach when it did except for notification from Vinny Troia of Night Lion Security—approximately 2 terabytes of information and data on 230 million people (and 110 million businesses) simply sat in public view.

10. The injuries suffered by Plaintiff and the proposed Classes as a direct result of the data breach include:

a. theft of their Personal Information and financial information;

b. costs for credit monitoring services;

c. unauthorized charges on their debit and credit card accounts;

[3] Exactis, *About Us*, http://www.exactis.com/about-us/ (last visited June 28, 2018)

d. the imminent and certainly impending 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's and Class members' Personal Information on the Internet black market;

e. the untimely and inadequate notification of the Data Breach;

f. the improper disclosure of their Customer Data;

g. loss of privacy;

h. 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;

i. ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. 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,

l. 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, imposition of withdrawal and purchase limits on compromised accounts, changing the information used to verify their identity to information not subject to this Data Breach, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

11. Herein, Plaintiff, individually and on behalf of the members of the Class and Subclass he seeks to represent, brings this action against Exactis. Plaintiff asserts claims for himself and on behalf of a nationwide class of consumers for Defendant's negligence, negligence per se, and unjust enrichment, and, for himself and on behalf of state-specific subclass, for Defendant's violation of state consumer protection and/or privacy laws. Plaintiff seeks monetary damages, declaratory and injunctive relief, and other remedies for violations of federal and state statutes and the common law.

II. JURISDICTION AND VENUE

12. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action, including claims asserted on behalf of a nationwide class and multiple state classes, filed under Rule 23 of the Federal Rules of Civil Procedure; there are likely millions of proposed Class members; the aggregate amount in controversy exceeds the jurisdictional amount of $5,000,000.00; and Defendant is a citizen of a State different from that of at least one Plaintiff. This Court also has subject-matter jurisdiction over Plaintiff's and Class (and Subclass) members' claims pursuant to 28 U.S.C. § 1367(a).

13. Venue is proper in this District under 28 U.S.C. § 1391 (a)–(d) because, inter alia, Defendant Exactis' principal place of business is located in the District, substantial parts of the events or omissions giving rise to the claim occurred in the District, and/or a substantial part of property that is the subject of the action is situated in the District. A substantial part of Plaintiff's personalactivities that Defendant collected, obtained, maintained, and allowed to be accessed without authorization during the data breach, occurred in or was found in the District. Also, Plaintiff is a resident of this District. And, a significant part of the risk of harm that Plaintiff now faces through Defendant's wrongful conduct is present in this District. Venue is also proper in the Jacksonville Division because Defendant is located here. *See* Rule 1.02, Local Rules for the United States District Court, Middle District of Florida.

III. PARTIES

A. Plaintiff.

14. Kenneth Heretick is a resident of Pinellas County, Florida.

B. Defendant.

15. Exactis is a United States Corporation with its principal place of business located at 1 Florida Park Drive S, Suite #308, Palm Coast, Florida 32137, which is located in Flagler County, Florida.

16. Exactis is a data aggregation firm that provides multi-channel consumer and business marketing data and marketing lists.

IV. STATEMENT OF FACTS

A. Defendant's Data Collection and Business Practices

17. Exactis collects information on people and sells it to businesses and marketers.[4]

[4] Exactis, *About Us*, http://www.exactis.com/about-us/ (last visited June 28, 2018)

18. Exactis boasts as having one of the largest such databases, and uses this database to assist companies create profiles on its customers.[5]

B. Exactis had Notice of Data Breaches Involving Exfiltration of Personal Information from Databases and Computer Systems

19. Defendant was well aware of the likelihood and repercussions of cyber security threats, including data breaches, having observed numerous other well-publicized data breaches involving major corporations over the last few years alone—including Equifax and Facebook—as well as the numerous other similar data breaches preceding those blockbuster breaches.

20. In September 2015, credit reporting agency Experian acknowledged that an unauthorized party accessed one of its servers containing the names, addresses, dates of birth, driver's license, and additional Personal Information of more than 15 million consumers over a period of two years.[6]

21. In March 2018, numerous media and news outlets broke blockbuster stories concerning Cambridge Analytica's exfiltration of user data from Facebook's platform.[7]

C. Exactis Failed to Comply with Industry Standards

22. Following the Equifax data breach, Senator Elizabeth Warren commissioned an investigation and, in February 2018, Senator Warren's office released the results of the 5-month investigation, setting fourth a number of findings regarding Equifax's data breach, including the inadequate data security practices that contributed to the data breach (the "Warren Report").[8]

---

[5] Exactis, *About Us*, http://www.exactis.com/about-us/ (last visited June 28, 2018)

[6] Reem Nasr, *Experian data breach hits more than 15M T-Mobile customers, applicants*, CNBC Tech (October 1, 2015) https://www.cnbc.com/2015/10/01/experian-reports-data-breach-involving-info-for-more-than-15m-t-mobile-customers.html

[7] Marisa Schultz, *Facebook's data breach could be higher than 85m: Cambridge Analytica whistleblower*, New York Post, (April 8, 2018) https://nypost.com/2018/04/08/facebooks-data-breach-could-be-higher-than-87m-cambridge-analytica-whistleblower/

[8] The Office of Senator Elizabeth Warren, *Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information* (February 2018) (available at: https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf) (last visited June 28, 2018)

23. Senator Warren's investigation revealed that the Equifax data breach was made possible because Equifax adopted weak cyber security measures that failed to protect consumer data and information falling within the Personal Information at issue in this Class Action.[9]

24. Senator Warren consulted with industry experts, and the Warren Report concluded that companies that hold large amounts of sensitive data—including Personal Information at issue here—should have multiple layers of cyber security, including: (a) frequently updated tools to prevent hackers from breaching their systems; (b) controls that limit hackers' ability to move throughout their systems in the event of an initial breach; (c) restrictions on hackers' ability to access sensitive data in the event of an initial breach; and (d) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible.[10]

25. Much like Exactis, Senator Warren warned that "Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures."[11]

26. Other cyber security analysts also found additional failures in Equifax's security measures, including failure to make use of firewalls that serve as a second line of defense.[12]

27. Despite these well-publicized Senate and other expert reports, Defendant failed to heed the recommendations, and inexplicably left its server—and the Personal Information which rested thereon—vulnerable and available to even the most basic cyber attack.

---

[9] Warren Report, at 3.
[10] Warren Report, at 3.
[11] Warren Report, at 3.
[12] Amos Ndegwa, *What is a Web Application Firewall?*, MAXCDN (May 31, 2016), https://www.maxcdn.com/one/visual-glossary/web-application-firewall/; Tushar Richabadas, *WAF Prevents Massive Data Breach at Equifax - The headline that could have been, but wasn't*, BARRACUDA (Sept. 22, 2017).

D. The Exactis Data Breach

28. In June of 2018, security researcher Vinny Troia, of Night Lion Security used Shodan, a search engine that allows a user to find computers and databases connected to the internet, to search for ElasticSearch databases visible on publicly accessible servers with American IP addresses.[13]

29. Much to Mr. Troia's surprise, Defendant Exactis' database containing the personal information of approximately 230 million individuals (as well as 110 million companies) was one of the results.[14]

30. Upon closer inspection, Mr. Troia discovered that not only was this database completely visible to public searches, but the database, containing close to 230 million individual records and approximately 2 terabytes in size, was unprotected by even a password-protected firewall or any form of encryption (the "Data Breach").[15]

31. The information contained in the unsecured database subject to this Data Breach included people's phone numbers, home and email addresses, personal interests and preferences, ages and genders of their children, and other extremely detailed, personal information—exceeding as many as 400 data points on each business and consumer ("Personal Information").[16]

32. This Personal Information was compromised due to Defendant's acts and omissions, as well as its failures to properly protect and secure the Personal Information, despite

---

[13] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, Wired (June 27, 2018) https://www.wired.com/story/exactis-database-leak-340-million-records/

[14] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, Wired (June 27, 2018) https://www.wired.com/story/exactis-database-leak-340-million-records/

[15] Andy Greenberg, *Marketing Firm Exactis Leaked a Personal Info Database with 340 Million Records*, Wired (June 27, 2018) https://www.wired.com/story/exactis-database-leak-340-million-records/

[16] Abrar Al-Heeti, *Exactis said to have exposed 340 millions records, more than Equifax breach*, CNET, (June 27, 2018) https://www.cnet.com/news/exactis-340-million-people-may-have-been-exposed-in-bigger-breach-than-equifax/

being aware of recent data breaches impacting other information and data gatherers, including Facebook, Equifax, and other prominent companies.

33. 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 months, if not longer.

34. Hackers and other nefarious actors, therefore, had months—if not longer—to collect this Personal Information unabated. During this time, Defendant failed to recognize the failure to protect this Personal Information. Timely action by Defendant likely would have significantly reduced the consequences of the Data Breach. Instead, Defendant took time to realize this Personal Information remained public and unsecured, and thus contributed to the scale of the Data Breach and the resulting damages.

35. 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.

36. 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.

37. Alarmingly, as of the filing of this Class Action Complaint, Defendant has yet to acknowledge the nature and extent of the Data Breach.

E. The Exactis Data Breach Caused Harm and Will Result in Additional Fraud

38. Without detailed disclosure to the 230 million affected people, including Plaintiff, the Nationwide Class members, and the Subclass members, these people have been left exposed, unknowingly and unwittingly, for months to continued misuse and ongoing risk of misuse of

their Personal Information without being able to take necessary precautions to prevent imminent harm.

39. Plaintiff has incurred costs associated with purchasing credit monitoring services.

40. The ramifications of Defendant's failures to keep Plaintiff's, the Nationwide Class members, and Subclass members' Personal Information secure are severe.

41. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[17] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[18]

42. Personal Information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have Personal Information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[19]

43. Identity thieves can use personal information, such as that of Plaintiff's, the other Nationwide Class members', and Subclass members', which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's Personal Information to obtain government benefits; or filing a fraudulent tax return using the victim's Personal Information to obtain a fraudulent refund.

---

[17] 17 C.F.R § 248.201 (2013).
[18] *Id.*
[19] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 10, 2017).

44. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[20]

45. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[21]

46. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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 continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

47. Thus, Plaintiff, the other Nationwide Class members, and Subclass members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Nationwide Class and Subclass are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

---

[20] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 10, 2017).

[21] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited June 28, 2018).

[22] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited June 28, 2018).

F. Plaintiff and the other Nationwide Class and Subclass Members Suffered Damages

48. Plaintiff's, the other Nationwide Class members', and the Subclass members' Personal Information is private and sensitive in nature, and was left inadequately protected, if not completely unprotected, by Defendant. Defendant did not obtain Plaintiff's, the other Nationwide Class members', and the Subclass members' consent to disclose their Personal Information to any other person or entity, as required by applicable law and industry standards.

49. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's, the other Nationwide Class members', and the Subclass members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's, the other Nationwide Class members', and the Subclass members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

50. Defendant had the resources to prevent a breach. Defendant made significant expenditures to market its products and touted its data security as industry leading, but neglected to adequately invest in data security, despite the growing number of Personal Information exfiltrations, as well as several years of well-publicized data breaches.

51. Had Defendant remedied the deficiencies in its database and computer systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would not have placed the Personal Information unencrypted on a public server, and instead would have prevented the dissemination of Personal Information and, ultimately, the theft of 230 million users' Personal Information.

52. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff, the other Nationwide Class members, and Subclass members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing the information used to verify their identity to information not subject to this Data Breach, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a company's slippage, as is the case here.

53. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's, the other Nationwide Class members', and the Subclass 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:

a. theft of their Personal Information and financial information;

b. costs for credit monitoring services;

c. unauthorized charges on their debit and credit card accounts;

d. the imminent and certainly impending 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's and Class members' Personal Information on the Internet black market;

e. the untimely and inadequate notification of the Data Breach;

f. the improper disclosure of their Customer Data;

g. loss of privacy;

h. 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;

i. ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. 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,

l. 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, imposition of withdrawal and purchase limits on compromised accounts, changing the information used to verify their identity to information not subject to this Data Breach, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

54. Although the Personal Information of Plaintiff, the other Nationwide Class Members, and the Subclass members has been stolen, Defendant continues to hold Personal Information of 230 million people, including Plaintiff's, the other Nationwide Class members', and the Subclass members' Personal Information. 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 Nationwide Class members, and Subclass 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.

V. CLASS ALLEGATIONS

55. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts that common law claims against Defendant for negligence, negligence per se, bailment, and unjust enrichment, declaratory and injunctive relief, and the various consumer protection laws, on behalf of himself and the following nationwide class ("the Nationwide Class" or the "Class"):

NATIONWIDE CLASS:

All residents of the United States whose Personal Information was contained in the publicly-accessible database and compromised as a result of the Data Breach.

56. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts statutory claims under state consumer protection statutes and state data breach statutes, on behalf of separate statewide subclass for Florida (the "Subclass"), defined as follows:

STATEWIDE FLORIDA SUBCLASS:

All residents of Florida whose Personal Information was contained in the publicly-accessible database and compromised as a result of the Data Breach.

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

58. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The members of the Nationwide Class and Subclass are so numerous and geographically dispersed that individual joinder of all Nationwide Class and Subclass members is impracticable. Plaintiff is informed and believes—based on the size of the exposed database—that there are over 230 million Class members. Those individuals' names and addresses are available from Defendant's records, and Nationwide Class and Subclass 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.

59. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual class members, including, without limitation:

a. Whether Defendant knew or should have known that its database, and the Personal Information stored thereon, was publicly-accessible;

b. Whether Defendant knew or should have known that its database, and the Personal Information stored thereon, was unencrypted;

c. Whether Defendant failed to take adequate and reasonable measures to ensure the database was protected;

d. Whether Defendant failed to take available steps to prevent and stop the Data Breach from happening;

e. Whether Defendant failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard the Personal Information;

f. Whether Defendant failed to provide timely and adequate notice of the Data Breach;

g. Whether Defendant owed a duty to Plaintiff and the other Nationwide Class and Subclass Members to protect their Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and the other Nationwide Class and Subclass Members;

h. Whether Defendant breached its duties to protect the Personal Information of Plaintiff, the other Nationwide Class, and Subclass Members by failing to provide adequate data security and by failing to provide timely and

accurate notice to Plaintiff, the other Nationwide Class members, and Subclass Members of the Data Breach;

i. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of millions of consumers' Personal Information;

j. Whether Defendant's conduct renders it liable for negligence, negligence per se, and unjust enrichment;

k. Whether, as a result of Defendant's conduct, Plaintiff and the other Nationwide Class and Subclass Members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

l. Whether, as a result of Defendant's conduct, Plaintiff and the other Nationwide Class and Subclass Members are entitled to injunctive, equitable, declaratory, and/or other relief, and, if so, the nature of such relief.

60. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the other Nationwide Class and Subclass members' claims because Plaintiff and the other Nationwide Class and Subclass members were subjected to the same allegedly unlawful conduct and damaged in the same way.

61. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate class representatives because his interests do not conflict with the interests of the other Nationwide Class and Subclass members who he seeks to represent,

Plaintiff has retained counsel competent and experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously. The Nationwide Class' and Subclass' interests will be fairly and adequately protected by Plaintiff's and his counsel.

62. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** The prosecution of separate actions by individual Nationwide Class and Subclass members would create a risk of inconsistent or varying adjudications with respect to individual Nationwide Class and Subclass members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications, which would be dispositive of the interests of other Nationwide Class and Subclass members and impair their interests. Defendant has acted and/or refused to act on grounds generally applicable to the Nationwide Class and Subclass, making final injunctive relief or corresponding declaratory relief appropriate.

63. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Nationwide Class and Subclass members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Nationwide Class and Subclass members to individually seek redress for Defendant's wrongful conduct. Even if Nationwide Class and Subclass members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast,

the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CLAIMS ALLEGED ON BEHALF OF THE NATIONWIDE CLASS

FIRST CAUSE OF ACTION

NEGLIGENCE
(Asserted by Plaintiff, individually, and on behalf of the Nationwide Class, and, in the alternative, Statewide Subclass)

64. Plaintiff, individually and on behalf of the other Nationwide Class and Subclass members, repeats and realleges Paragraphs 1 through 63, as if fully alleged herein.

65. Defendant owed a duty to Plaintiff and the other Nationwide Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure that Plaintiff's and the other Nationwide Class and Subclass members' Personal Information in Defendant's possession was adequately secured and protected. Defendant further owed a duty to Plaintiff and the other Nationwide Class and Subclass members to implement processes that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

66. Defendant owed a duty to Plaintiff and the other Nationwide Class and Subclass members to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the Personal Information of Plaintiff and the other Nationwide Class and Subclass members about whom Defendant collected, maintained, and used such information.

67. Defendant owed a duty of care to Plaintiff and the other Nationwide Class and Subclass members because they were foreseeable and probable victims of any inadequate security practices. Defendant solicited, gathered, and stored the Personal Information provided by Plaintiff and the other Nationwide Class and Subclass members to facilitate its products to customers. Defendant knew it inadequately safeguarded such information on its computer systems and knew or should have known that such information was publicly-accessible and not subject to any reasonable data security measures.

68. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC 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 Personal Information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty.

69. Defendant knew that a breach of its systems would cause damages to Plaintiff and the other Nationwide Class and Subclass members, and Defendant had a duty to adequately protect such sensitive Personal Information.

70. Defendant owed a duty to timely and accurately disclose to Plaintiff and the other Nationwide Class and Subclass members that their Personal Information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiff and the other Nationwide Class and Subclass members could take appropriate measures to cancel or change usernames and passwords on compromised accounts, change the information used to verify their identity to information not

subject to this Data Breach, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services and take other steps to mitigate or ameliorate the damages caused by Defendant's misconduct.

71. Defendant knew, or should have known, of the risks inherent in collecting and storing the Personal Information of Plaintiff and the other Nationwide Class and Sublcass members, and of the critical importance of providing adequate security of that information.

72. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and the other Nationwide Class and Subclass members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping and maintenance of the Personal Information of Plaintiff and the other Nationwide Class and Subclass members.

73. Defendant breached the duties it owed to Plaintiff and the other Nationwide Class and Subclass members by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the Personal Information of Plaintiff and the other Nationwide Class and Subclass members.

74. Defendant breached the duties it owed to Plaintiff and the other Nationwide Class and Subclass members by failing to properly implement technical systems or security practices that could have prevented the dissemination and loss of the Personal Information at issue.

75. Defendant breached the duties it owed to Plaintiff and the other Nationwide Class and Subclass members by failing to properly maintain their sensitive Personal Information.

Given the risk involved and the amount of data at issue, Defendant's breach of its duties was entirely unreasonable.

76. Defendant breached its duties to timely and accurately disclose that Plaintiff's and the other Nationwide Class and Subclass members' Personal Information in Defendant's possession had been or was reasonably believed to have been, stolen or compromised.

77. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the other Nationwide Class and Subclass members, their Personal Information would not have been compromised.

78. The injury and harm suffered by Plaintiff and the other Nationwide Class and Subclass members, as set forth above, was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Nationwide Class and Subclass members' Personal Information within Defendant's possession. Defendant knew or should have known that its systems and technologies for processing, securing, safeguarding and deleting Plaintiff's and the other Nationwide Class and Subclass members' Personal Information were inadequate, publicly accessible, and vulnerable to being breached by hackers.

79. Plaintiff and the other Nationwide Class and Subclass members suffered injuries and losses described herein as a direct and proximate result of Defendant's conduct resulting in the Data Breach, including Defendant's lack of adequate reasonable and industry standard security measures. Had Defendant implemented such adequate and reasonable security measures, Plaintiff and the other Nationwide Class and Subclass members would not have suffered the injuries alleged, as the Data Breach would likely have not occurred.

80. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the other Nationwide Class and Subclass members have suffered injury and the significant risk of harm in the future, and are entitled to damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(Asserted by Plaintiff, individually, and on behalf of the Nationwide Class, and, in the alternative, Statewide Subclass)

81. Plaintiff, individually and on behalf of the other Nationwide Class and Subclass members, repeats and realleges Paragraphs 1 through 63, as if fully alleged herein.

82. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies—such as Defendant—of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Defendant's duty.

83. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach.

84. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

85. The Nationwide Class and the alternative state specific subclass are within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce, and Defendant bears primary responsibility for reimbursing consumers for fraud losses. Plaintiff and absent class members are consumers.

86. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff, the Nationwide Class, and the alternative state specific class members.

87. As a direct and proximate result of Defendant's negligence per se, the Plaintiff, the Nationwide Class and the alternative state specific class members have suffered and continue to suffer injury, including but not limited to:

a. theft of their Personal Information and financial information;

b. costs for credit monitoring services;

c. unauthorized charges on their debit and credit card accounts;

d. the imminent and certainly impending 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's and Class members' Personal Information on the Internet black market;

e. the untimely and inadequate notification of the Data Breach;

f. the improper disclosure of their Customer Data;

g. loss of privacy;

h. 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;

i. ascertainable losses in the form of deprivation of the value of their Personal Information, for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. 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

l. 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, imposition of withdrawal and purchase limits on compromised accounts, changing the information used to verify their identity to information not subject to this Data Breach, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

THIRD CAUSE OF ACTION

UNJUST ENRICHMENT
(Asserted by Plaintiff, individually, and on behalf of the Nationwide Class, and, in the alternative, Statewide Subclass)

88. Plaintiff, individually and on behalf of the other Nationwide Class and Subclass members, repeats and realleges Paragraphs 1 through 63, as if fully alleged herein.

89. Defendant collected, maintained, and sold Plaintiff's, the other Nationwide Class and Subclass members', and others' Personal Information without the knowledge or direct consent of Plaintiff, the other Nationwide Class members, the Subclass members, and others.

90. Defendant appreciates or has knowledge of the benefits conferred directly upon them by Plaintiff, the other Nationwide Class members, Subclass members, and others.

91. As a result of Defendant's wrongful conduct, as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff, the other Nationwide Class members, the Subclass members, and others.

92. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's, the other Nationwide Class members', and Subclass members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

93. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff, the other Nationwide Class members, the Subclass members, and others, in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

94. Plaintiff, the other Nationwide Class members, the Subclass members, and others did not confer these benefits officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these wrongfully obtained profits.

95. Defendant is therefore liable to Plaintiff, the other Nationwide Class members, and the Subclass members for restitution in the amount of the benefit conferred on Defendant, including specifically Defendant's wrongfully obtained profits.

FORTH CAUSE OF ACTION

DECLARATORY AND INJUNCTIVE RELIEF
(Asserted by Plaintiff, individually, and on behalf of the Nationwide Class, and, in the alternative, Statewide Subclass)

96. Plaintiff, individually and on behalf of the other Nationwide Class members, repeats and realleges Paragraphs 1 through 95, as if fully alleged herein.

97. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described in this Complaint.

98. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's common law, statutory, and other duties to reasonably safeguard Plaintiff's, the other Nationwide Class members', the Subclass members', and others' Personal Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff, the other Nationwide Class members, the Subclass members, and others from further data breaches that compromise their Personal Information. Plaintiff alleges that Defendant's data security measures were and remain inadequate. Furthermore, Plaintiff continues to suffer injury

as a result of the compromise of their Personal Information, and remain at imminent risk that further compromises of his Personal Information will occur in the future.

99. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed and continues to owe a legal duty to secure Plaintiff's, the other Nationwide Class members', the Subclass members', and others' Personal Information, and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Defendant continues to breach its legal duties by failing to employ reasonable measures to secure Plaintiff's, the other Nationwide Class members', the Subclass members', and others' Personal Information.

100. The Court also should issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect Plaintiff's, the other Nationwide Class members', the Subclass members', and others' Personal Information.

101. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendant's database and other computer systems. The risk of another such data breach is real, immediate, and substantial.

102. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Exactis, Plaintiff will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable data security measures is relatively minimal, and Defendant has pre-existing legal obligations to employ such measures.

103. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's database, thus eliminating the additional injuries that would result to Plaintiff, the other Nationwide Class members, the Subclass members, and others whose Personal Information would be further compromised.

VII. STATE CONSUMER PROTECTION LAWS BROUGHT BY THE STATEWIDE SUBCLASS

FIFTH CAUSE OF ACTION

VIOLATIONS OF FLORIDA'S DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Florida Statute Section 501.201, *et seq.*
(Asserted by Plaintiff, individually, and on behalf of the Statewide Subclass)

104. Plaintiff, individually and on behalf of the other Statewide Subclass members, repeats and realleges Paragraphs 1 through 95, as if fully alleged herein.

105. Plaintiff, and members of the statewide Subclass (the "Class" for purposes of this claim), are individuals who have had their Personal Information collected, stored, and sold by Defendant.

106. The purpose of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, et seq., ("FDUTPA") is to "protect the consuming public...from those who engage in unfair methods of competition, or unconscionable, deceptive or unfair acts or practice in the conduct of any trade or commerce." Fla. Stat. § 501.202(2).

107. Plaintiff is both a "consumer" as defined by Fla. Stat. § 501.203(7), as well as a person, generally referenced in the FDTUPA, and the subject transaction is "trade or commerce" as defined by Florida Statute § 501.203(8).

108. FDUPTA was enacted to protect the consuming public and legitimate business enterprises from those who engage in unconscionable, deceptive, or unfair acts or practices in the

conduct of any trade or commerce, and in unfair methods of competition. For the reasons discussed herein, Defendant violated FDUPTA by engaging in the unconscionable, deceptive, unfair acts or practices described herein and proscribed by Florida Statutes §§ 501.201, *et seq*., and 501.171, *et seq.*, as well as those acts proscribed by Section 5 of the FTC Act.

109. Defendant's unconscionable, deceptive, and unfair acts and practices described herein were likely to, and did in fact, deceive members of the public, including consumers and persons (like Plaintiff) acting reasonably under the circumstances and to their detriment. In committing the acts alleged herein, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by failing to timely notify Florida residents of the Data Breach, which constitutes an unfair or deceptive trade practice in the conduct of commerce in violation of FDUPTA. Fla. Stat. §§ 501.201, *et seq.*, 501.171, *et seq.*

110. Defendant's actions constitute unconscionable, deceptive, and unfair acts or practices because, as alleged herein, Defendant knew or reasonably should have known that Plaintiff's and the Class members' Personal Information was accessed, and Defendant is required by law to timely notify Plaintiff and the Class members that their Personal Information was accessed. Fla. Stat. § 501.171(4).

111. Additionally, Defendant violated Section 5 of the FTC Act, and therefore FDUTPA, by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach.

112. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices, proscribed by Florida law.

113. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other members of the Class have been harmed, in that they were not notified of the Data Breach, which resulted in profound vulnerability to their Personal Information and other financial accounts.

114. Plaintiff reserves the right to allege other violations of FDUPTA as discovery unfolds and as Defendant's conduct is ongoing. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff has been damaged and is entitled to recover actual damages, to the extent permitted by law, including Fla. Stat. § 501.211, in an amount to be proven at trial.

115. In addition, pursuant to Fla. Stat. § 501.211, Plaintiff seeks equitable relief and to enjoin Defendant on terms the Court considers reasonable. Plaintiff also seeks reasonable attorneys' fees and costs, as prescribed by §§ 501.211(2) Florida Statutes (2009).

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Nationwide Class and Subclass members, respectfully requests the Court enter judgment in his favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's attorneys as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiff and the other Nationwide Class and Subclass Members actual, direct (where actual and direct damages are separate under the law), compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits Defendant received as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, and punitive or exemplary damages, to the extent permitted by law;

6. That the unlawful acts alleged in this Complaint be adjudged and decreed to be unconscionable, deceptive, and unfair acts and practices in violation of the FDUTPA;

7. That the unlawful acts alleged in this Complaint be adjudged and decreed to be negligent, negligent per se, and unjust enrichment;

8. That Plaintiff be granted the declaratory relief sought herein;

9. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, including fees and expenses;

10. That the Court award pre- and post-judgment interest at the maximum legal rate; and

11. That the Court grant all such other relief as it deems just and proper.

[Remainder of Page Intentionally Left Blank]

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial on all claims so triable.

Dated: June 28, 2018

Respectfully submitted,

/s/ John A. Yanchunis

John A. Yanchunis
Florida Bar No. 324681
Ryan J. McGee
Florida Bar No. 64957
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
jyanchunis@ForThePeople.com
rmcgee@ForThePeople.com

Adam J. Levitt (*Pro hac vice* to be submitted)
Amy E. Keller (*Pro hac vice* to be submitted)
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602
Tel: (312) 214-7900
alevitt@dlcfirm.com
akeller@dlcfirm.com

Mark Abramowitz (*Pro hac vice* to be submitted)
Justin Hawal (*Pro hac vice* to be submitted)
DICELLO LEVITT & CASEY LLC
7556 Mentor Ave
Mentor, Ohio 44060
Tel: (440) 953-8888
mabramowitz@dlcfirm.com
jhawal@dlcfirm.com

Stuart A. Davidson
Florida Bar No. 84824
Christopher C. Gold
Florida Bar No. 88733
ROBBINS GELLER RUDMAN &
DOWD LLP
120 East Palmetto Park Road
Suite 500

Boca Raton, Florida 33432
Telephone: (561) 750-3000
Facsimile: (561) 750-3364
sdavidson@rgrdlaw.com
cgold@rgrdlaw.com

Counsel for Plaintiff and the Proposed Nationwide Class and Subclass

ClassAction.org