

FILED

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA

2017 NOV 20 PM 4:49

CLERK OF COURT
MIDDLE DISTRICT OF FLORIDA
TALLAHASSEE, FLORIDA

SHELLEY FOREMAN, on behalf of)
herself and all others similarly situated,)

Plaintiff,)

v.)

SOLERA HOLDINGS, INC.,)

Defendant.)

Civil Action No.: 6:17-cv-2002-OLL-37DCI

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Shelley Foreman, individually and on behalf of all others similarly situated, by and through her counsel, bring this action against Defendant Solera Holdings, Inc., (“Defendant” or “Solera”), and alleges as follows based upon personal knowledge, investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. Defendant provides risk management and asset protection software and services to the automotive industry and property insurance marketplace. In the United States, Defendant operates through its subsidiaries: AudaExplore, Hollander, Identifix, AutoPoint, DST, LYNX Services, APU and ENSERVIO.

2. On or about April 14, 2017, Defendant sent a letter to its current and former employees advising that their 2016 W-2 tax form information had been subjected to “a data compromise”¹

3. The letter explained that the “source” of the “data compromise was a phishing

¹ A copy of the April 14, 2017 letter (the “Notice”) is attached hereto as Exhibit A.

email that was sent to one of our employees.” In response to the email, that employee provided information “relating to employees’ 2016 Form W-2s.”

4. Falling for a well-known “phishing” or scam email scheme which human resources and accounting professionals have been warned about, the Solera employee complied with an email request to send unknown cyber criminals an unencrypted data file which contained either copies of W-2 statements or all of the sensitive personally identifying information (“PII”) needed to fill out a W-2, including names, mailing addresses, Social Security numbers, and wage and withholding information (the “Data Disclosure”). The compromised data contained PII for W-2 employees² (as categorized by the Internal Revenue Service (“IRS”)) who worked at and received wages from Solera during the time period of January 1, 2016 through December 31, 2016.

5. As a consequence of the Data Disclosure, Class Members have suffered damages by taking measures to both deter and detect identity theft. Class Members have been required 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 Disclosure on their lives including, *inter alia*; placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, scheduling and attending appointments with the IRS, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, 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

² In simplest terms, the IRS has two categories for workers: employees and independent contractors. For employees, payroll taxes are automatically deducted from paychecks and paid to the government through the employer. The employer reports the wages to the IRS at the end of the year on a W-2 form. Independent contractors are responsible for calculating and submitting their own payroll taxes. Companies report the wages paid to independent contractors on a Form 1099. See, *IRS Publication 15-A, available at <https://www.irs.gov/publications/p15a/ar02.html>* (last visited November 8, 2017).

compensable: indeed, 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 an employer's slippage, as is the case here.

6. Without question the PII of Plaintiff and Class members, particularly their Social Security numbers and wage and tax information, was taken for purposes of identity theft, and unfortunately, Solera's current and former employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud.

7. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

8. Plaintiff brings this class action against Solera for failing to adequately secure and safeguard the PII of Plaintiff and the Class, for failing to comply with industry standards regarding electronic transmission of PII, and for failing to provide timely accurate and adequate notice to Plaintiff and other Class members as to precisely how and when their sensitive personal information had been given to unknown persons.

9. Solera disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the data it stores was safeguarded, failing to take available steps to prevent the disclosure from happening, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data even for internal use. As the result, the PII of Plaintiff and Class Members was compromised and disclosed to an unknown and unauthorized third party. However, as this same information remains stored in Solera computer systems, Plaintiff and Class members have an interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Shelley Foreman

10. Plaintiff Shelly Foreman is a citizen and resident of Palm Coast, Florida.

11. Ms. Foreman is a former employee at Solera whose PII was disclosed without her authorization to an unknown third party as a result of the Data Disclosure.

12. Ms. Foreman worked for Solera in Daytona, Florida for a division of its AutoPoint subsidiary.

13. Prior to the Data Disclosure, Ms. Foreman had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

14. It was not until around April 14, 2017, that Ms. Foreman learned from the Notice that a Solera employee had been responsible for emailing Ms. Foreman's PII to an unknown, unauthorized third party.

15. In May 2017, Ms. Foreman received a letter from the IRS about a tax transcript that had been requested using her personal, identifying information. Ms. Foreman had not requested her tax transcript, nor did her husband, and thus she knew it had been fraudulently requested. Ms. Foreman spent time speaking with the IRS and informing them that the tax transcript had been fraudulently requested. The IRS informed Ms. Foreman, that as a result of the identity theft resulting in the fraudulent tax transcript request, Ms. Foreman is not permitted to file her taxes electronically for at least several years. This will continue to cause Ms. Foreman to spend increased time and expenses to file her taxes and will result in delay of any refunds. In the same month, \$10,000 was taken fraudulently through two separate transactions from account that Ms. Foreman held jointly with her mother. Ms. Foreman spent several weeks working with her bank to resolve this theft, which required closing the account and going through the process

of opening new one. A representative with the bank's fraud department and a personal banker at one of the local branches expressed their opinion that the fraudulent access to the account would have been possible as a result of the amount and type of personal information compromised in the Data Disclosure. Until this incident, neither Ms. Foreman nor her mother had ever had suspicious or fraudulent activity on any of their bank accounts.

16. Afraid that this type of theft could easily happen again given that her personal information remains in the hands of criminals due to the Data Disclosure, Ms. Foreman now spends time every day checking her banking accounts online.

17. After the data disclosure, Ms. Foreman also received a credit monitoring alert that someone attempted to fraudulently open a financial account in her name. Ms. Foreman spent time looking into this notification and checking her report to ensure no other accounts had been opened in her name fraudulently.

18. As a result of the Data Disclosure, Ms. Foreman has spent, and will continue to spend, numerous hours monitoring her tax information, bank accounts, and credit reports and taking other actions necessary to protect herself from future incidents of identity theft or fraud.

Defendant

19. Defendant Solera Holdings, LLC is a company with its principal place of business in Westlake, Texas.

JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and a citizen of a foreign state.

21. This Court has personal jurisdiction over Defendant because the Defendant is authorized to and do conduct substantial business in the state of Florida, and in this District.

22. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendant regularly conducts business in this District, Plaintiff resides in this District and a substantial part of the events or omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

23. As a condition of employment, Solera requires that employees entrust it with certain personal information. In its ordinary course of business, Solera maintains personal and tax information, including the name, address, zip code, date of birth, wage and withholding information, and Social Security number, of each current and former employee.

24. Plaintiff and members of the proposed Class, as current and former employees, relied on Solera to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

25. On Monday, March 13, 2017, Solera learned that some of its employees had experienced fraudulent 2016 income tax returns filed in their names.³ On Friday, March 31, 2017, Solera notified Attorneys General across the country of the breach and provided them a copy of a notice that Solera allegedly was “sending out... to Solera employees.”⁴

26. On or about April 14, 2017, Solera sent a letter to current and former employees, advising that Solera and “its affiliated companies” had a “security incident” in which “an

³ Notice of Data Breach letter provided to New Hampshire Attorney General from attorneys of Solera Holding, Inc. dated March 31, 2017, available at <https://www.doj.nh.gov/consumer/security-breaches/documents/solera-20170331.pdf> (last visited November 11, 2017).

⁴ *Id.* See also, Notice of Data Breach letter provided to Oregon Attorney General from attorneys of Solera Holding, Inc. dated March 31, 2017, available at <https://justice.oregon.gov/consumer/DataBreach/Home/GetBreach/1066549897> (last visited November 11, 2017).

unauthorized individual impersonating a Solera executive requested [by email] certain information relating to employees' 2016 Form W-2s.... before it was determined that the request was fraudulent, the employee provided the requested information.”⁵ Additionally, the letter stated that “employees of Solera reported receiving alerts from the IRS that fraudulent 2016 income tax returns had been filed in their names.”

27. The letter stated that the employees' 2016 W-2 tax information, including names, addresses, social security numbers and wage information, work email addresses and the EIN's of certain Solera group companies had been involved in the breach.

28. The April 14, 2017 letter was the first notice received by Solera's current and former employees that their information had been wrongly disclosed.

29. The letter failed to advise of the date of the Data Disclosure, or why Solera waited until mid-April, almost a month after discovering the incident, to notify employees of the Data Disclosure.

30. The Data Disclosure occurred at a time in the calendar year when W-2 information is most vital and valuable.

31. Solera could have prevented this Data Disclosure. Solera was not without warning of this phishing email scam, which was publicly available, yet it failed to implement adequate measures to protect its employees' PII.

⁵ Notice of Data Breach letter provided to Washington Attorney General from attorneys of Solera Holding, Inc. dated May 5, 2017, attaching copy of April 14, 2017 letter sent to employees, *available at* http://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Safeguarding_Consumers/Internet_Safety/Breach%20Solera%20Holdings%20Inc%202017-05-05.pdf (last visited November 11, 2017).

32. Solera's negligence in safeguarding its employees' PII is exacerbated by the repeated warnings and alerts, not only of the increasing risk of general email scams, but of the actual W-2 phishing email scam it chose to ignore and, thus, fell prey to.

33. On August 27, 2015, the Federal Bureau of Investigation ("FBI") issued a report warning of the increasingly common scam, known as Business Email Compromise, in which companies had fallen victim to phishing emails.⁶ Most importantly, this report called attention to the significant spike in scams, also referred to as spoofing, in which cyber criminals send emails that appear to have initiated from the CEO or other top-level executive at the target company.

34. Business Email Compromise or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A telltale sign of a spoofing e-mail is an "urgent" request from a company "executive" requesting that confidential information be provided via email.

35. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name."⁷

36. Spoofing fraud has been steady increasing in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received

⁶ See, *Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), available at <https://www.ic3.gov/media/2015/150827-1.aspx> (last visited November 8, 2017).

⁷ Brian Krebs, *FBI: \$2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), available at <http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/> (last visited November 8, 2017).

reports from over 17,000 victims of “spoofing” scams, which resulted in more than \$2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.⁸

37. Companies can mount two primary defenses to spoofing scams: employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal and tax information.

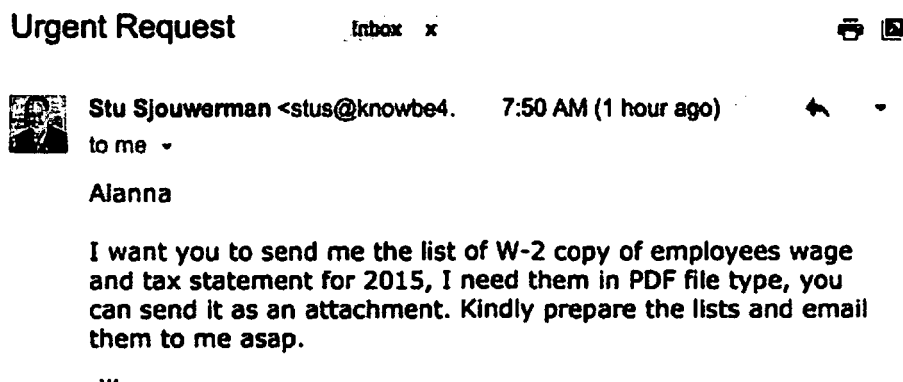
38. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

39. On February 24, 2016, cybersecurity journalist Brian Krebs warned of the precise scam which snared Solera in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.⁹ Krebs warned that cybercriminals were attempting to scam companies by

⁸ *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), available at <https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-email-scams> (last visited November 8, 2017).

⁹ Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, KREBS ON SECURITY available at <http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/> (last visited November 8, 2017).

sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company:



40. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. In precise detail, the alert stated:

The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.

The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

“This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments,” said IRS Commissioner John Koskinen. “If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming

the identity of people requesting personal information about employees.”¹⁰

41. Again on January 25, 2017, the IRS renewed the alert specifically cautioning, “company payroll officials to double check any executive-level or unusual requests for lists of Forms W-2 or Social Security number.”¹¹

42. A simple phone call to verify this request would have prevented the Data Disclosure.

43. Simply encrypting the file containing the PII would have prevented the Data Disclosure.

44. Despite the widespread prevalence of spoofing aimed at obtaining confidential information from employers and despite the warnings of the W-2 email scam from the 2015 tax season and renewed alerts for the 2016 tax season, Solera provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure.

45. Solera failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

- a. How to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

¹⁰ IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (March 1, 2016), available at <https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s> (last visited November 8, 2017).

¹¹ IRS, *IRS, States and Tax Industry Renew Alert about Form W-2 Scam Targeting Payroll, Human Resource Departments*, IR-2017-10 (Jan. 25, 2017), available at: <https://www.irs.gov/uac/newsroom/irs-states-and-tax-industry-renew-alert-about-form-w2-scam-targeting-payroll-human-resource-departments> (last visited November 8, 2017).

- b. Effective password management and encryption protocols for internal and external emails;
- c. Avoidance of responding to emails that are suspicious or from unknown sources;
- d. Locking, encrypting and limiting access to computers and files containing sensitive information;
- e. Implementing guidelines for maintaining and communicating sensitive data; and
- f. Protecting sensitive employee information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

46. Solera's failures handed criminals the PII of Plaintiff and other Class Members and put Plaintiff and the Class at serious, immediate and ongoing risk for identity theft and fraud.

47. Access to W-2 information permits identity thieves to quickly and easily file fraudulent tax returns, using the victim's information to obtain a fraudulent refund. The IRS will direct deposit the refund to the bank account or prepaid debit card (which are virtually untraceable) provided by the thief.

48. The Data Disclosure was caused by Solera's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Solera failed to comply with security standards and allowed its employees' PII to be compromised by failing to implement security measures that could have prevented or mitigated the Data Disclosure. Solera failed to implement even the most basic of security measures to require encryption of any data file containing PII sent electronically, even internally within the company.

49. Solera failed to ensure that all personnel in its human resources and payroll departments were made aware of this well-known and well-publicized phishing email scam.

50. Upon discovery, Solera failed to take reasonable steps to clearly and conspicuously inform Plaintiff and the other Class Members of the nature, timing and extent of the Data Disclosure. By failing to provide adequate timely notice, Solera prevented Plaintiff and Class Members from protecting themselves from the consequences of the Data Disclosure.

51. The ramifications of Solera's failure to keep its employees' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹² The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹³

53. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

¹² 17 C.F.R. § 248.201 (2013).

¹³ *Id.*

54. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.¹⁴

55. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

56. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

57. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."¹⁵

58. Based on the foregoing, the information compromised in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data

¹⁴ Social Security Administration, Identity Theft and Your Social Security Number, *available at* <http://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited December 30, 2016).

¹⁵ *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited November 8, 2017).

breach such as those that occurred at Target and Home Depot, because, there, victims could cancel or close credit and debit card accounts. The information compromised in the Solera Data Disclosure is impossible to “close” and difficult, if not impossible, to change—Social Security number, name, employment information, income data, etc.

59. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁶

60. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police during an arrest.

61. The fraudulent activity resulting from the Data Disclosure may not come to light for years.

62. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII 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.¹⁷

¹⁶ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited November 8, 2017).

¹⁷ GAO, Report to Congressional Requesters, at 29 (June 2007), available at <http://www.gao.gov/new.items/d07737.pdf> (last visited November 8, 2017).

63. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

64. Despite all of the publicly available knowledge of the continued compromises of PII, and alerts regarding the actual W-2 phishing email scam perpetrated, Solera's approach to maintaining the privacy of its employees PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

65. Solera has failed to provide compensation to Plaintiff and Class Members victimized in this Data Disclosure. Solera has not offered to provide any assistance or compensation for the costs and burdens – current and future - associated with the identity theft and fraud resulting from the Data Disclosure. Solera has not offered employees any assistance in dealing with the IRS or state tax agencies.

66. It is incorrect to assume that reimbursing a consumer for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, 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."¹⁸

67. To date, Solera has offered its employees only two years of credit monitoring service through Experian. The offered service is inadequate to protect the Plaintiff and Class Members from the threats they face, particularly in light of the PII stolen.

¹⁸ Victims of Identity Theft, 2012 (Dec. 2013) at 10, 11, *available at* <https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited November 8, 2017).

68. As a result of Solera's failures to prevent the Data Disclosure, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

- a. Unauthorized use and misuse of their PII;
- b. The loss of the opportunity to control how their PII is used;
- c. The diminution in value of their PII;
- d. The compromise, publication and/or theft of their PII;
- e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- f. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- g. Delay in receipt of tax refund monies;
- h. Lost opportunity and benefits of electronically filing of income tax returns;
- i. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- j. The continued risk to their PII, which remains in the possession of Solera and is subject to further breaches so long as Solera fail to undertake appropriate measures to protect the PII in their possession; and
- k. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure

for the remainder of the lives of Plaintiff and Class Members.

69. As a direct and proximate result of Solera's wrongful actions and inaction and the resulting Data Disclosure, Plaintiff and Class 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 B Disclosure reach 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, and filing police reports. This time has been lost forever and cannot be recaptured.

70. In all manners of life in this country, time has constantly been recognized as compensable, for many people it is the way they are compensated. Plaintiff and Class members should be free of having to deal with the consequences of Solera's slippage.

71. The injuries to the Plaintiff and Class members were directly and proximately caused by Solera's failure to implement or maintain adequate data security measures for its employees' PII.

CLASS ACTION ALLEGATIONS

72. Plaintiff brings this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

73. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

All current and former Solera employees whose PII was compromised as a result of the Data Disclosure.

74. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiff seeks to represent the following state classes only in the event that the Court declines to certify the Nationwide Class above. Specifically, the state class consists of the following:

All current and former Solera employees who currently reside in Florida and whose PII was compromised as a result of the Data Disclosure.

75. Excluded from the Classes are the officers, directors and legal representatives of Solera and the judges and court personnel in this case and any members of their immediate families.

76. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, it is estimated to be at or above 4000. The exact number is generally ascertainable by appropriate discovery as Solera had knowledge of the employees whose PII was in the data file it disclosed.

77. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). 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 and to what extent Solera had a duty to protect the PII of Class members;
- b. Whether NSC had a duty to not disclose the PII of Class Members to unauthorized third parties;
- c. Whether NSC had a duty to not use the PII of Class Members for non-business purposes;
- d. Whether Solera failed to adequately safeguard the PII of Class members;

- e. Whether Solera adequately, promptly, and accurately informed Class Members that their PII had been compromised;
- f. Whether Solera failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;
- g. Whether Solera engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class members;
- h. Whether Class members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Solera' wrongful conduct;
- i. Whether Plaintiff and the members of the Class are entitled to restitution as a result of Solera' wrongful conduct; and,
- m. Whether Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

78. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff' claims are typical of those of other Class Members because Plaintiff's PII, like that of every other class member, was disclosed by Solera. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

79. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of

interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intend to prosecute this action vigorously.

80. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporate Solera. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical.

81. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each member of the

Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

82. The litigation of the claims brought herein is manageable. Defendant' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

83. Adequate notice can be given to Class Members directly using information maintained in Solera's records.

84. Unless a Class-wide injunction is issued, Solera may continue in its failure to properly secure the PII of Class Members, Solera may continue to refuse to provide proper notification to Class Members regarding the Data Disclosure, and Solera may continue to act unlawfully as set forth in this Complaint.

85. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

86. 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, using, and safeguarding their PII;

- b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant and the Class and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately, and accurately informed Class Members that their PII had been compromised;
- g. 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 Disclosure;
- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members; and,
- i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Class)

87. Plaintiff restates and realleges paragraphs 1-86 above as if fully set forth herein.

88. As a condition of their employment, employees were obligated to provide Solera with certain PII, including their date of birth, mailing addresses and Social Security numbers.

89. Plaintiff and the Class Members entrusted their PII to Solera on the premise and with the understanding that Solera would safeguard their information, use their PII for business

purposes only, and/or not disclose their PII to unauthorized third parties.

90. 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.

91. Solera knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its employees' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

92. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing Defendant security protocols to ensure that Plaintiff and Class members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of employees' personal and tax information.

93. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Solera knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiff and the Class.

94. Solera's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Solera misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Solera misconduct also included

its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiff and Class Members.

95. Plaintiff and the Class Members had no ability to protect their PII that was in Solera possession.

96. Solera was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Disclosure.

97. Solera had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within its possession might have been compromised, how it was compromised and precisely the types of information that were compromised and when. Such notice was necessary to allow Plaintiff and the Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

98. Solera had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

99. Solera has admitted that the PII of Plaintiff and Class Members was wrongfully disclosed to unauthorized third persons as a result of the Data Disclosure.

100. Solera, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Solera possession or control.

101. Solera improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

102. Solera failed to heed industry warnings and alerts issued by the IRS to provide

adequate safeguards to protect employees' PII in the face of increased risk of a current phishing email scheme being perpetrated.

103. Solera, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its employees' PII.

104. Solera, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence, and scope of the Data Disclosure.

105. But for Solera's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

106. There is a close causal connection between Solera failure to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

107. As a result of Solera's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: identity theft, out-of-pocket expenses associated with addressing false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Class)

108. Plaintiff restates and realleges paragraphs 1-86 above as if fully set forth herein.

109. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

110. Defendant owed a duty to its employees, including Plaintiff and Class Members, to keep their PII contained as a part thereof, confidential.

111. Defendant intentionally released to unknown and unauthorized third parties an unencrypted file containing the PII of Plaintiff and Class Members.

112. Defendant intentionally allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiff and Class Members.

113. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiff and Class Members, especially where the information includes Social Security numbers and wage information, would be highly offensive to a reasonable person.

114. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Solera as part of their employment, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their authorization.

115. The Data Disclosure at the hands of Defendant constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a

reasonable person.

116. As a proximate result of the above acts and omissions of Solera, the PII of Plaintiff and Class Members was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

117. Unless and until enjoined, and restrained by order of this Court, Solera wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Solera can be viewed, distributed and used by unauthorized persons. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Class)

118. Plaintiff restates and realleges paragraphs 1-86 above as if fully set forth herein.

119. Plaintiff and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to Solera as a condition of their employment.

120. Implicit in the employment agreement between the Solera and its employees was the obligation that Solera would use the PII of its employees for business purposes only and not make unauthorized disclosures of the information.

121. Solera had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses.

122. Additionally, Solera implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

123. Plaintiff and Class members fully performed their obligations under the implied contract with Solera. Solera did not.

124. Solera breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff' and Class members' PII, which was compromised as a result of the Data Disclosure.

125. Solera acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their PII as a condition of employment in exchange for compensation and benefits.

126. As a direct and proximate result of Solera breach of its implied contacts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remain in Solera possession and is subject to further unauthorized disclosures so long as Solera fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its 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 Disclosure for the remainder of the lives of Plaintiff and Class members.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Class)

127. Plaintiff restates and realleges paragraphs 1-85 above as if fully set forth herein.

128. In light of the special relationship between Solera and its employees, whereby Solera required Plaintiff and Class Members to provide highly sensitive, confidential, personal and financial information as a condition of their employment, Solera was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiff and Class members, for the safeguarding of employees' PII and wage information.

129. Solera had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their employer/employee relationship, in particular to keep secure income records and the PII of its employees.

130. Solera breached its duty of care to Plaintiff and Class members to ensure that their PII and W-2 data was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by voluntarily disclosing the information, in an unencrypted format, to an unknown and unauthorized third party.

131. As a direct and proximate result of the Solera actions alleged above, the Plaintiff and Class members have suffered actual damages.

FIFTH CAUSE OF ACTION
Violation of State Unfair and Deceptive Trade Practices Acts
(On Behalf of the Class)

132. Plaintiff restates and realleges paragraphs 1-85 above as if fully set forth herein.

133. Solera engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Disclosure occurred through the use of email, an instrumentality of interstate commerce.

134. As alleged herein this Complaint, Solera engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

- a. failure to implement data security practices to safeguard PII;
- b. failure to use employees' PII for business purposes only;
- c. failure to make only authorized disclosures of employees' PII; and
- d. failure to timely and accurately disclose the Data Disclosure to Plaintiff and Class members.

135. Speedway's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Solera engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former employees.

136. In committing the acts alleged above, Solera engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former employees that it did not follow industry best practices for the collection, use, and storage of PII.

137. As a direct and proximate result of Solera's conduct, Plaintiffs and other members of the Class have been harmed and have suffered damages including, but not limited to: identity theft; damages arising from identity theft; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and

restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

138. 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, declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all others similarly situated, pray for relief as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;
- B. A mandatory injunction directing Solera to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;
- C. A mandatory injunction requiring that Solera provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PII to unauthorized persons;
- D. For an award of damages, in an amount to be determined;
- E. For an award of attorneys' fees and costs;
- G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: November 17, 2017

Respectfully submitted,

/s /John A. Yanchunis

JOHN A. YANCHUNIS
jyanchunis@ForThePeople.com
MARISA GLASSMAN
mglassman@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

JEAN SUTTON MARTIN*
jean@jsmlawoffice.com
LAW OFFICE OF JEAN SUTTON
MARTIN PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (910) 292-6676
Facsimile: (888) 316-3489

Attorneys for Plaintiff and the Proposed Class

* *pro hac vice* application to be submitted



Franchise Tax Account Status

As of : 11/17/2017 14:28:05

This Page is Not Sufficient for Filings with the Secretary of State

SOLERA HOLDINGS, INC.

Texas Taxpayer Number 12611038162

Mailing Address 1301 SOLANA BLVD STE 2100 BLDG 2
WESTLAKE, TX 76262-1675

Right to Transact Business in Texas ACTIVE

State of Formation DE

Effective SOS Registration Date 06/04/2015

Texas SOS File Number 0802228578

Registered Agent Name CORPORATION SERVICE COMPANY DBA
CSC - LAWYERS INCO

Registered Office Street Address 211 E. 7TH STREET, SUITE 620 AUSTIN, TX
78701

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS SHELLEY FOREMAN, on behalf of herself and all others similarly situated, (b) County of Residence of First Listed Plaintiff <u>Flagler County</u> (EXCEPT IN U.S. PLAINTIFF CASES) (c) Attorneys (Firm Name, Address, and Telephone Number) Morgan & Morgan Complex Litigation Group 201 N. Franklin Street, 7th Floor, Tampa, FL 33602 813.223.5505	DEFENDANTS SOLERA HOLDINGS, INC., County of Residence of First Listed Defendant _____ (IN U.S. PLAINTIFF CASES ONLY) NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED. Attorneys (If Known) _____
---	---

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)	III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)																								
<input type="checkbox"/> 1 U.S. Government Plaintiff <input type="checkbox"/> 2 U.S. Government Defendant <input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) <input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;"></td> <td style="width: 10%; text-align: center;">PTF</td> <td style="width: 10%; text-align: center;">DEF</td> <td style="width: 45%;"></td> <td style="width: 10%; text-align: center;">PTF</td> <td style="width: 10%; text-align: center;">DEF</td> </tr> <tr> <td>Citizen of This State</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 1</td> <td style="text-align: center;"><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business In This State</td> <td style="text-align: center;"><input type="checkbox"/> 4</td> <td style="text-align: center;"><input type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td style="text-align: center;"><input type="checkbox"/> 2</td> <td style="text-align: center;"><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business In Another State</td> <td style="text-align: center;"><input type="checkbox"/> 5</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> <td style="text-align: center;"><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> <td style="text-align: center;"><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF		PTF	DEF	Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input type="checkbox"/> 4	Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF		PTF	DEF																				
Citizen of This State	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input type="checkbox"/> 4																				
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

IV. NATURE OF SUIT (Place an "X" in One Box Only)				
CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	FORFEITURE/PENALTY <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act	BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609
REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	CIVIL RIGHTS <input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	PRISONER PETITIONS Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	OTHER STATUTES <input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes	

V. ORIGIN (Place an "X" in One Box Only)

1 Original Proceeding
 2 Removed from State Court
 3 Remanded from Appellate Court
 4 Reinstated or Reopened
 5 Transferred from Another District (specify)
 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
 28 U.S.C. § 1332(d)

Brief description of cause:
 Negligence, Invasion of Privacy, Breach of Implied Contract, Breach of Fiduciary Duty, FUDTPA

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.
 DEMAND \$ 5,000,000.00
 CHECK YES only if demanded in complaint:
 JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions):

JUDGE _____ DOCKET NUMBER _____

DATE 11/17/2017 SIGNATURE OF ATTORNEY OF RECORD /s/ John A. Yanchunis

FOR OFFICE USE ONLY


RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

Exhibit A



1301 Solana Blvd.
Bldg. 2, Suite 2100
Westlake, TX 76262

April 14, 2017

Shelley Foreman


Dear Shelley,

We are writing to inform you of a security incident that may have affected certain personal information of current and former employees of Solera Holdings, Inc. and its affiliated companies ("Solera"). As a precaution, we would like to call your attention to steps you can take to help protect your information. We sincerely regret any concern this incident may cause.

What Happened?

Recently, certain employees of Solera reported receiving alerts from the IRS that fraudulent 2016 income tax returns had been filed in their names. Solera immediately formed an incident response team consisting of senior representatives from IT, legal, internal audit, and human resources, as well as external professional cyberthreat resources, to investigate whether the company had been impacted by a data security incident, determine the root cause and implement a remediation plan.

On April 9, 2017, our ongoing investigation confirmed that the source of the suspected data compromise was a phishing email that was sent to one of our employees. In that email, an unauthorized individual impersonating a Solera executive requested certain information relating to employees' 2016 Form W-2s. Unfortunately, before it was determined that the request was fraudulent, the employee provided the requested information.

Our investigation uncovered no evidence that this incident involved any wider unauthorized access to or use of any Solera computer system or network.

What Information Was Involved?

The information sent to the unknown perpetrator included your first and last name, home address, Social Security number, 2016 wage and deduction information, work email addresses, and the EINs of certain Solera group companies.

What We Are Doing

Solera takes the privacy and protection of personal information very seriously, and has previously taken various steps to try to prevent incidents like this at our company, including by sending out US-wide phishing awareness emails weeks before this incident occurred and previously implementing mandatory cyber security training for employees. We deeply regret that this incident occurred despite our preventative efforts.

We took steps to address this incident promptly after it was discovered, including convening an incident response team and engaging external advisors to perform a forensic investigation, notifying impacted persons, and reporting to the IRS, FBI, and other authorities.

What You Can Do

A new IRS unit dedicated to helping companies victimized by W-2 scams has been established, and we have notified this unit about the incident we experienced. While the IRS is taking steps to help protect you from tax-related fraud, we want to make you aware of additional steps you can take to guard against fraud or identity theft.

First, we have engaged Experian® to offer you complimentary fraud resolution and identity protection services for two years. These services help detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. To enroll, please follow these steps:

- Visit www.experianidworks.com/3bcreditone to enroll
- Provide the following activation code: **YM6S6Y28D**
- Enroll by 7.31.17 (your code will not work after this date)
- You may also enroll over the phone by calling 877-890-9332 between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **DB01417**.

Also note that the IRS recommends that you file your tax return as soon as possible each year. If the IRS sends you a request for additional information about your 2016 tax return, please respond immediately. To further protect your personal information, you may also wish to file a Form 14039 "Identity Theft Affidavit" with the IRS to help prevent someone from filing a fraudulent tax return in your name in future tax years. For additional information from the IRS for employees impacted by W-2 scams, visit www.irs.gov/identitytheft or call their Identity Theft Hotline at 1-800-908-4490. There may also be similar resources and forms to file for individual states, so you may wish to contact your state department of revenue directly for more information.

As an additional precautionary measure and good practice, you should carefully review your credit reports for suspicious activity, accounts you did not open, or inquiries from creditors you did not initiate. You should also remain vigilant and continue to monitor your reports for unusual activity going forward. If you see anything you do not understand on your credit report, call a credit agency immediately. If you find that unauthorized accounts were opened, you should also call your local police or sheriff's office, file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

Finally, please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

For more information about this incident, or if you have additional questions or concerns, you may contact us at the dedicated call center line we have established at (866) 578-5412. Again, we sincerely regret any concern this incident may cause you.

Sincerely,

Solera Holdings, Inc.

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Experian Membership: We have engaged Experian® to offer you complimentary fraud resolution and identity protection services for two years. You can contact Experian immediately in the event you experience any fraud to speak to an Identity Restoration Specialist (see below description). Be prepared to provide engagement number **DB01417** as proof of eligibility for the identity restoration services.

You have access to the following features once you activate your Experian membership:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet surveillance:** daily scanning of the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian online, please contact Experian's customer care team at 877-890-9332 by July 31, 2017.

A credit card is **not** required for enrollment in Experian IdentityWorks. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Review of Accounts and Credit Reports: As a precaution you may regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the end of this guide.

Remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the relevant institutions, the credit bureaus, the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, <http://www.riag.ri.gov>.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may request an extended fraud alert if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur

fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting agency. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion (www.transunion.com)
P.O. Box 1000
Chester, PA 19016
800-888-4213

Fraud Alerts:
<https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp>
Credit Freezes:
<https://www.freeze.equifax.com>

Fraud Alerts:
<https://www.experian.com/fraud/center.html>
Credit Freezes:
https://www.experian.com/consumer/security_freeze.html

Fraud Alerts:
<http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>
Credit Freezes:
<http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Solera Holdings Hit with Class Action Lawsuit Over 2016 Employee Tax Form 'Data Compromise'](#)
