

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

BECKY WELBORN and WENDY WINDRICH,
on behalf of themselves and all others similarly
situated,

Plaintiffs,

v.

INTERNAL REVENUE SERVICE, JOHN
KOSKINEN, in his official capacity as
Commissioner of Internal Revenue, and DOES 1
through 100, inclusive,

Defendants.

Case No.:

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Beck Welborn and Wendy Windrich (collectively, “Plaintiffs”), individually and on behalf of the proposed class described below, bring this action for injunctive relief, and actual and statutory damages against Defendants Internal Revenue Service (“IRS”) and Commissioner John A. Koskinen (“Koskinen” or “Commissioner”), and allege based on information and belief except as where indicated, as follows:

INTRODUCTION

1. This case arises out of the cyber-breach of IRS’s systems that resulted in cyber-criminals stealing the identity and financial information (“Personal Identification Information” or “PII”) from approximately 330,000 taxpayers, which would have been prevented, had the IRS fixed the known security deficits in its data storage system. At the time of the data breach of taxpayers’ information, the

IRS had received – but not acted on - numerous reports that its systems did not have adequate security; it knew its systems had been previously hacked by cyber-criminals; it knew that cyber-criminals were highly motivated to hack the IRS system in order to steal taxpayer information that has significant value in the black market; and it had actual knowledge that cyber-criminals were engaged in ongoing efforts to hack the IRS systems. Despite this knowledge, the IRS deliberately and intentionally decided not to implement the security measures needed to prevent the subject data breach.

2. Plaintiffs and Class members include the 330,000 Americans, as well as their spouses and dependants, who had their tax information stolen via the IRS’s “Get Transcript” online service, which allows taxpayers to access the IRS system to order copies of their own tax returns and other filings. That service, which allowed taxpayers to access the IRS system, did not have requisite security in place to prevent cyber-criminals from also accessing the IRS system. The impact of the breach extends beyond the 330,000 people directly affected, given that the personal information of spouses and dependents was also included in the stolen transcripts.

3. The IRS requires that taxpayers submit a significant amount of personal and financial information to the IRS. The IRS collects and maintains this personal and financial information on each taxpayer. The IRS also relies extensively on computerized systems to carry out its responsibilities to collect taxes, process tax returns, and enforce the federal tax laws. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of this sensitive information against unauthorized access or loss. Otherwise, taxpayers would be exposed to invasion of privacy and financial loss or damage from identity theft or other financial crimes, like what happened in May of this year.

4. The Government Accountability Office (“GOA”) and the Treasury Inspector General for Tax Administration (“TIGTA”) specially issued reports warning the IRS of its lax computer security

years before the hack of the 330,000 taxpayer accounts on the IRS's website. This is not a new threat, but has been known to the IRS for a number of years.

5. What should have been a trustworthy digital service had been compromised and is yet the latest sign that the U.S. Government cannot be relied upon to keep the personal data of its citizens safe. This information is highly valuable to criminals. Even though the theft began in February 2015, the criminal activity was apparently not detected until after tax season. According to Koskinen's testimony to the U.S. Senate Finance Committee¹ on June 2, 2015, *hackers made 200,000 attempts on the "Get Transcript" page, approximately half of which were successful.*² Since the theft, the IRS has taken the service offline.

6. The IRS's process for verifying people requesting transcripts is vulnerable to exploitation to fraudsters because it relies on static identifiers and so-called "knowledge-based authentication" (KBA) – i.e., challenge questions that can be easily defeated with information widely available for sale in the cybercrime underground and/or with a small amount of searching online. The IRS knew or should have known that KBA would not have provided adequate security for the taxpayer data.

7. The KBA questions—which involve multiple-choice "out of wallet" questions such as previous address, loan amounts and dates—can be successfully enumerated with random guessing or found on the Internet. For example, Zillow.com can provide answers to the KBA questions in a matter of minutes. Spokeo also solves the "old address" questions with 100% accuracy. Moreover, answers to common security questions such as "What is your mother's maiden name?" are easily gleaned from

¹ The Senate Committee on Finance stands alone, having legislative jurisdiction over the Internal

² In a statement released by the IRS on August 17, 2015, the agency announced that the personal information of more than 220,000 taxpayers had been stolen that the agency had originally estimated.

the public domain by using such non-sophisticated techniques as looking up a Facebook profile or engaging in a little light social engineering.

8. The hacks which took place on the IRS did not require significant funding, technology, or intelligence. The only necessary preconditions were knowledge that the application exists and the ability to deduce what information is required to access information in it. Once infiltrated, the cyber-criminal has access to the taxpayer's full tax transcript, including, identification information, children and spouse social security numbers, prior W2s, current W2s, income, holdings, and more than enough information to fraudulently file for a tax refund using the taxpayer's identification.

9. The gravity of the stolen data is alarming, as stated by Senator Ron Wyden at the hearing:

The thieves who steal taxpayer information could wipe out people's life savings and leave them in financial ruin. They could falsify tax returns next year or further down the road. They could take out huge, fraudulent home or student loans. And on a bigger scale, the money stolen in this cybercrime wave could be funneled into more criminal activity. It could wind up in war zones. There's a possibility that it could fund acts of terrorism without being traced.

10. At the June 2, 2015, hearing of the Senate Finance Committee after the breach, panel Chairman Orrin Hatch ("Hatch") told Koskinen that his agency "has failed" the taxpayers whose returns were stolen in the breach reported the prior month. Chairman Hatch added:

These taxpayers, and their families, must now begin the long and difficult process of repairing their reputations. And they must do so with the knowledge that the thieves who stole their data will likely try to use it to perpetrate further fraud against them.

11. Based on what Koskinen said repeatedly in congressional testimony³, the security breach was not related to the financial resources available to the agency. Instead, it was a deliberate decision not to implement the security measures recommended by GAO and TIGTA, and reportedly by its own employees.

12. According to an anonymous former IT manager for the IRS quoted by Patrick Thibodeau in *Computerworld*, security staff “would have preferred to implement a more dynamic and aggressive security framework that would have stopped the fraudsters from being able to get in using the information they stole from the third party,” but senior IRS leadership allegedly overruled them, choosing instead to roll out a more simple authentication method to encourage use.

13. Despite the IRS’s failure to comply with TIGTA’s recommendations and failure to take steps to secure its systems, the IRS went ahead and knowingly launched an application that it knew was vulnerable and insecure.

14. As such, Plaintiffs on behalf of themselves and others similarly situated allege that through its conduct Defendants violated the Privacy Act of 1974 and the Administrative Procedure Act. Plaintiffs request damages to compensate them for their current and future losses and injunctive relief to fix the IRS’s security protocol, implement TIGTA’s audit recommendations, implement President Obama’s executive order focused on improving the security of consumer financial transactions, to provide adequate credit monitoring services for a sufficient time period, and to provide after-the-fact identity repair services and identity theft insurance to protect Class members from fraud and/or identity theft.

³ “Not every problem is a budget problem, so I don’t want to wander around town every time we have a challenge saying, ‘Ah, if we had more money, we’d fix it,’” Koskinen said. “This is a technology issue, not a budget (issue), but a question of security, a question of keeping up criminals in terms of authentication.” Likewise, at the hearing, U.S. Senator Ron Wyden stated that the IRS’s inadequate security system “is not just a question of resources.”

PARTIES

A. Plaintiffs

15. Plaintiff Becky Welborn (“Welborn”) is a resident and citizen of Dripping Springs, Texas.

16. Plaintiff Wendy Windrich (“Windrich”) is a resident and citizen of Conroe, Texas.

B. Defendants

17. Defendant Internal Revenue Service is, and was at all times relevant hereto, an administrative agency of the United States Government, subject to the Administrative Procedures Act (“APA”). *See* 5 U.S.C. § 551. The IRS is headquartered at 1111 Constitution Avenue, NW, Washington, DC 20224.

18. Defendant John A. Koskinen is being sued in his official capacity as the Commissioner of Internal Revenue. He serves as the head of the Internal Revenue Service, in Washington, DC.

JURISDICTION

19. This Court has subject matter jurisdiction over all claims in this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different than Defendants’ state of citizenship, the amount in controversy exceeds \$5 million, and the proposed class includes in excess of 100 members.

20. This Court also has subject matter jurisdiction over the Privacy Act of 1974 claim pursuant to 5 U.S.C. § 552a(g)(1).

21. This Court has personal jurisdiction over the IRS because it maintains headquarters in the District of Columbia and the relevant conduct occurred in the District of Columbia.

22. This Court has personal jurisdiction because Defendant Commissioner Koskinen performs his official duties in the District of Columbia and the relevant conduct occurred in the District of Columbia.

23. Venue is proper in this Court under 28 U.S.C. § 1391(e) because this is an action against officers and agencies of the United States; Defendant Internal Revenue Service is found in this judicial district; Defendant Commissioner Koskinen performs his official duties in this judicial district; and a substantial part of the events or omissions giving rise to this action occurred in this judicial district.

FACTUAL ALLEGATIONS

A. The Internal Revenue Service Is Responsible for the Collection and Storage of a Substantial Amount of Confidential and Sensitive Personnel Records

24. The IRS is an agency in the U.S. Department of the Treasury responsible for administering the United States tax code. The official mission statement of the IRS is to:

Provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all.

25. The IRS employs approximately 91,000 employees, who collected over \$3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued \$374 billion in tax refunds during Fiscal Year 2014. Part of the duties of the IRS include investigating individuals who use the IRS as a means of furthering fraudulent, criminal activity that negatively impacts the operations of the IRS.

26. The current Commissioner of the IRS is John Koskinen, who was confirmed by the Senate on December 20, 2013. The Commissioner of Internal Revenue presides over the nation's tax system. The Commissioner "ensures that the agency maintains an appropriate balance between taxpayer service and tax enforcement and administers the tax code with fairness and integrity." The Commissioner is "responsible for establishing and interpreting tax administration policy and for

developing strategic issues, goals and objectives for managing and operating the IRS. The Commissioner is responsible for overall planning, directing, controlling and evaluating IRS policies, programs, and performance.”

27. One of the responsibilities of the Commissioner of the IRS is to provide taxpayers and tax professionals with electronic products and services that they desire to enable them to interact and communicate with the IRS. This is rooted in the IRS’s acknowledgement that the current technology environment has raised taxpayers’ expectations for online customer service interactions and the IRS’s need to meet these expectations. The self-assisted interactive online tool, “Get Transcript” application, which can include account transactions, line-by-line tax return information, and income reported to the IRS, was one of the applications born of this vision.

28. As part of an effort to provide taxpayers with self-service and electronic service options in the form of web-based tools, the IRS launched the Get Transcript online application in January 2014. Get Transcript allows taxpayers to view and print a copy of their prior-year tax information, also known as a transcript, in a matter of minutes. Taxpayers use tax transcript information for a variety of financial activities, such as verifying income when applying for a mortgage or a student loan.

29. To access Get Transcript, taxpayers go through an authentication process to establish their identity. The authentication process includes several “out-of-wallet” questions, which are designed to elicit information that only the taxpayer would normally know, but which can be easily ascertained by a third party. The taxpayer then receives an email from the Get Transcript system containing a confirmation code that they enter to access the application and request a transcript.

B. The IRS Generally Knew that its Systems Would be a Target for Cyber-Criminals

30. The IRS was aware of the recent surge in massive data breaches experienced by large corporations such as Home Depot, Chase Bank, Target, Sony, Premera Blue Cross, Anthem Blue

Cross, and the United States Office of Personnel and Management. As the result of these massive data breaches, government agencies such as the IRS knew or should have known that its systems storing taxpayers' personal data were at a very high risk of being hacked by cybercriminals.

31. In the past two years alone, well over 100 million people have received a letter, call or email notifying that they have been victims of a data breach. In some cases, key personal data has been exposed by retailers, including Target; for others, it is health insurance companies including Anthem, or employers like Sony.

32. Over the past year alone, millions of people have fallen prey to identity theft through massive data breaches at some of the nation's largest companies. The following are examples of the largest data breaches in recent times:

- In September 2014, Home Depot, the world's largest home improvement chain, confirmed that a total of 56 million credit and debit cards were affected by a data breach;
- In June and July 2014, JP Morgan Chase, the nation's largest bank by assets, confirmed that it had experienced a massive data breach that affected 76 million households and 7 million small businesses;
- In early December 2014, Sony's system was hacked, resulting in the theft of 47,000 social security numbers, which subsequently appeared more than 1.1 million times on 601 publicly-posted files stolen by hackers;
- In January 2014, it was revealed that Target Corporation's holiday data breach affected up to 70 million people, who had their names, mailing addresses, phone numbers, and email addresses stolen by hackers;

- In January 2015, it was revealed that health insurance giant Premera Blue Cross experienced a data breach involving the personal data of approximately 80 million members across the country.
- In February 2015, Anthem, Inc., the country's second largest health insurer, announced that its systems had been compromised in a massive data breach, in which a total of 78.8 million records were stolen, including 8.8 to 18.8 million records of non-customers.
- In June 2015, the United States Office of Personnel and Management announced that its systems housing employee records had been breached by cybercriminals, resulting in a loss of sensitive data for approximately 14 million employees.

C. The IRS's Specifically Knew that its Cyber Security Measures Were Inadequate to Prevent Cyber-Criminals from Hacking into its System and Stealing Taxpayer Information

33. The Federal Information Security Management Act of 2002 ("FISMA")⁴ was enacted to strengthen the security of information and systems within federal government agencies. The IRS collects and maintains a significant amount of personal and financial information on each taxpayer. As custodians of taxpayer information, the IRS has an obligation to protect the confidentiality of sensitive information against unauthorized access or loss.

34. As part of the FISMA legislation, the Offices of Inspectors General are required to perform an independent evaluation of each agency's information security programs and practices. Under FISMA, an agency must develop, implement, and maintain a security program that assesses the

⁴ At the time the IRS audits were conducted, the Federal Information Security Management Act of 2002 governed the auditing process. 44 U.S.C. § 3541 *et seq.* TIGTA submitted the most recent audit report in September 2014. The President signed the Federal Information Security Modernization Act of 2014 into law on December 18, 2014. The Federal Information Security Modernization Act updates and supersedes the Federal Information Security Management Act. For purposes of this Complaint, "FISMA" means the Federal Information Security Management Act of 2002 and "Modernization Act" means the Federal Information Security Modernization Act of 2014.

risks and provides adequate security for the operations and assets of programs and software systems under its control. Specifically, FISMA requires: (1) annual agency program reviews; (2) annual Inspector General evaluations; (3) agency reporting to the Office of Management and Budget (“OMB”) the results of Inspector General evaluations for unclassified software systems; and (4) an annual OMB report to Congress summarizing the material received from agencies. The OMB uses the reports to help it ensure that the various federal agencies are in compliance with its cyber security requirements.

35. In July 2010, OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security* (DHS), expanded the role of the DHS in regard to the operational aspects of federal agency cybersecurity and information systems that fall within FISMA requirements. The DHS prepares the security metrics to assist the federal agencies and the Inspectors General in evaluating agency progress in achieving compliance with federal security standards.

36. FISMA oversight of the Department of the Treasury is performed by two distinct Inspector General Offices: the Treasury Inspector General for Tax Administration (TIGTA) and the Treasury Office of the Inspector General (OIG). The TIGTA is responsible for oversight of the Internal Revenue Service (IRS), while the Treasury OIG is responsible for all other Treasury bureaus.

37. To assist the Inspectors General in evaluating federal agencies’ compliance with the FISMA, the DHS issued the Fiscal Year (FY) 2014 *Inspector General Federal Information Security Management Act Reporting Metrics* on December 2, 2013, which specified 11 information security program areas and listed specific attributes within each area for evaluation. The 11 information security program areas are: (1) continuous monitoring management; (2) configuration management; (3) identity and access management; (4) incident and response reporting; (5) risk management;

(6) security training; (7) plan of action and milestones; (8) remote access management; (9) contingency planning; (10) contractor systems; and (11) security capital planning.

38. In accordance with FISMA, the TIGTA is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of the IRS. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that it provides the taxpayer with assurance that the approximately 91,000 IRS employees perform their duties in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse. Over the past year, a significant part of TIGTA's workload has been devoted to investigating scams that can negatively impact the integrity of tax administration.

39. TIGTA identified a number of areas in which the IRS should better protect taxpayer data and improve its overall security posture. Most recently, in its FISMA report for Fiscal Year 2014, TIGTA found four security program areas were not fully effective due to one or more DHS guideline program attributes that were not met:

- Continuous Monitoring Management. The IRS has not yet implemented its Information Security Continuous Monitoring (ISCM) strategy, but stated that it is fully participating in the DHS's Continuous Diagnostics and Mitigation Program to comply with the OMB M-14-033 mandate to implement ISCM and is in the process of determining its final toolset to meet the program requirements.
- Incident Response and Reporting. The IRS did not always report incidents involving Personally Identifiable Information to the U.S. Computer Emergency Response Team (US-CERT) within established time frames.

- Security Training. The IRS has not yet fully implemented a process for identifying and tracking contractors who are required to complete specialized training, but stated that it continues to make progress and is working to incorporate a clause into contracts that requires contractors to complete and record such training.
- Remote Access Management. The IRS has not fully implemented unique user identification and authentication that complies with Homeland Security Presidential Directive-12 (HSPD-12).

40. Two security program areas, Configuration Management and Identity and Access Management, did not meet the level of performance specified by the DHS guidelines due to the majority of the specified attributes not being met.

41. “Identity and Access Management” ensures that only those with a business need are able to obtain access to IRS systems and data. However, TIGTA found that the IRS needed to fully implement unique user identification and authentication that complies with Department of Homeland Security directives, ensure that users are only granted access based on needs, ensure that user accounts are terminated when no longer required, and control the improper use of shared accounts.

42. “Configuration Management” ensures that settings on IRS systems are maintained in an organized, secure, and approved manner, including timely updating “patches”⁵ to known security vulnerabilities. TIGTA found that the IRS needed to improve enterprise-wide processes for assessing configuration settings and vulnerabilities by means of automated scanning, timely remediating scan result deviations, timely installing software patches, and controlling changes to hardware and software configurations.

⁵ A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

43. Patch management is an important element in mitigating the security risks associated with known vulnerabilities to computer systems. This is critical to prevent intrusions by unauthorized individuals or entities. Due to its importance, TIGTA evaluated the effectiveness of the IRS security patch management process, which, according to TIGTA, has been “an ongoing challenge for the IRS.” TIGTA found that the IRS had not yet implemented key patch management policies and procedures needed to ensure that all IRS systems are patched timely and operating securely.

44. According to Treasury Inspector George’s testimony, “Any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over vulnerable computers and get access to the sensitive data the computer systems may contain, including taxpayer data.”

45. TIGTA warned in its 2014 audit that “[u]ntil the IRS takes steps to improve its security program deficiencies and fully implements all 11 security program areas required by the FISMA, taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected.”

46. Furthermore, in March of this year, IT security journalist Brian Krebs warned that the IRS’s process for verifying the identities of people requesting a tax transcript was vulnerable to exploitation because it relied on knowledge-based questions whose answers could be found through public records, stolen credit reports, or leaked personal information –which is exactly what occurred.

D. The IRS Deliberately and Intentionally Chose Not to Implement Appropriate Security of Taxpayer Information

47. Since Fiscal Year 2011, TIGTA has designated the security of taxpayer data as the top concern facing the IRS based on the increased number and sophistication of threats to taxpayer information and the need for the IRS to better protect taxpayer data and improve its enterprise security

program. In compliance with FISMA requirements, TIGTA's investigators audit the IRS's security systems every year and suggest improvements.

48. To provide oversight of the IRS's Information Security Program, TIGTA completes approximately seven audits each year on various security programs, systems, and solutions. As of March 2015, these audits have resulted in 44 recommendations that the IRS has thus far failed to implement. While most of these recommendations are based on recent audits, there are 10 recommendations from five security audits that were completed during the Fiscal Years of 2008-2012.

49. Some of the oldest recommendations that were made, but never implemented by the IRS, were recommendations that TIGTA believed have had some bearing on the IRS's ability to stop or prevent the Get Transcript breach.

50. The IRS's Computer Security Incident Response Center ("CSIRC") is responsible for monitoring IRS networks 24 hours a day year-round for cyber attacks and responding to various computer security incidents. Prior to the security breach, TIGTA evaluated the effectiveness of the CSIRC at preventing, detecting, reporting, and responding to computer security incidents targeting IRS computers and data. TIGTA found that the CSIRC was deficient in certain respects. At the time of their review, TIGTA found that the CSIRC's host-based intrusion detection system was not monitoring a significant percentage of IRS servers, which leaves that portion of the IRS network and data at risk. In addition, CSIRC was not reporting all computer security incidents to the Department of the Treasury, as required. Finally, incident response policies, plans, and procedures were either nonexistent, inaccurate, or incomplete.

51. TIGTA has also previously raised concerns over the remediation of security weaknesses identified in their audits to the IRS. TIGTA reviewed closed corrective actions to security weaknesses and findings reported by TIGTA and identified weak management controls in the IRS over its closed

planned corrective actions for the security of systems involving taxpayer data. During the audit, TIGTA determined that eight (42%) of 19 planned corrective actions that were approved and closed by the IRS as fully implemented in response to reported security weaknesses from prior TIGTA audits were not in fact fully implemented.

52. Moreover, according to TIGTA, “management control” also involves the use of risk-based decisions by IRS management to make an exception to its own policies and requirements based on appropriate justification and a thorough assessment of evident and potential risks. Exceptions related to security information systems are permissible if meeting the requirement is: (1) not technically or operationally possible, or (2) not cost effective. TIGTA found that these risk-based decisions were not adequately tracked and documented. Without required supporting documentation, TIGTA “could not determine why decisions were made and whether the information technology risks were appropriately accepted and approved.”

53. According to TIGTA, patch management is an important element in mitigating the security risks associated with known vulnerabilities to computer systems because it is critical to prevent intrusions by unauthorized individual or entities. Due to its importance, TIGTA evaluated the effectiveness of the IRS security patch management process, which has been an ongoing challenge for the IRS. TIGTA found that the IRS had not implemented key patch management policies and procedures needed to ensure that all IRS systems are patched timely and operating securely. TIGTA warned that any significant delays in patching software with critical vulnerabilities provides ample opportunity for persistent attackers to gain control over vulnerable computers and get access to the sensitive data the computer systems may contain, including taxpayer data. The IRS failed to patch the software as recommended and thereby allowed the attackers to gain access to taxpayer data through its “Get Transcript” application.

54. At the Finance Committee hearing, Senator Pat Roberts stated that “[i]t’s a paradox of enormous irony” that just weeks prior to this breach, privacy experts briefed his staff on how safe the Get Transcript application was. Senator Roberts observed that this is not a new threat, because the IRS, the Inspector General, GAO, and the oversight agencies, have been concerned about and warned the IRS of these vulnerabilities. Senator Roberts also noted that “[i]n a rush to push out programs, like Get Transcript, we have let access and purported cost savings overtake the absolute need to safeguard taxpayer information.”

55. Moreover, in October 2014, President Barak Obama issued an executive order focused on improving the security of consumer financial transactions. In Section 3 of the order, titled “Securing Federal Transactions Online,” the President directed the National Security Staff, the White House Office of Science and Technology Policy, and Office of Management and Budget to present a plan “consistent with the guidance set forth in the 2011 National Strategy for Trusted Identifiers in Cyberspace [NSTIC], to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.”

56. Following that order, a group of government agencies submitted a plan to the President that would “ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.” When President Obama signed that executive order, it certainly applied to the IRS and getting online identity – and identity protection – right should have been the IRS’ priority.

57. When Get Transcript was initiated, the IRS was the lone exception to every other federal agency in offering online access to sensitive information. Other agencies, which often had two or three services that should have been online, refused to do so because of the high level of risk in identity

authentication. When Get Transcript launched, it was known, in the private and public sectors, that the username/password mechanism, like that used for Get Transcript, was broken and insecure. Despite such knowledge, the IRS went live with the insecure application anyway.

E. The IRS Breach Caused Damage to the Plaintiffs and Putative Class

58. During the 2015 filing season, taxpayers used the Get Transcript application to obtain approximately 23 million copies of their recently filed tax information. During the middle of May 2015, the IRS's cybersecurity team noticed unusual activity on the Get Transcript application. At the time, the cybersecurity team thought it may be a "denial of service" attempt, where hackers try to disrupt a website's normal functioning. However, after looking deeper into the issue, it was discovered that there were questionable attempts to access the Get Transcript application. As a result, the IRS shut down the Get Transcript application on May 21, 2015. Further investigation by the IRS initially revealed that a total of approximately 200,000 suspicious attempts to gain access to taxpayer information on the Get Transcript application were made between mid-February and mid-May, with more than half being successful attempts. Just recently, however, on August 17, 2015, the IRS announced that the theft of American taxpayer data was much worse than originally thought and has revised the number of successful stolen forms to 330,000, or three times the amount initially reported.

59. According to reports from the IRS, an individual or individuals succeeded in clearing its authentication process. Although the illegal activity began in February 2015, the IRS did not detect the malicious activity until mid-May 2015. According to the most recent information provided by the IRS, approximately 610,000 taxpayers, including spouses and children of the taxpayers, have had access attempts to their PII, with 330,000 of those actually compromised.

60. As the taxpayer information remains at large and in the hands of cybercriminals, Plaintiffs and the putative class are at great risk of the cybercriminals using their PII for fraudulent

purposes that will harm Plaintiffs and the putative class. The possibilities for which the thieves can profit from the stolen personal tax information are limitless, in time and money.

F. Implementation of Proper Security Measures that the IRS Intentionally Elected Not to Employ Would Have Prevented the Loss to Taxpayers

61. The Government Accountability Office (“GAO”) issued a report in March 2015 that identified more than 50 weaknesses in the IRS's computer security that had not been resolved. In the report, the GAO stated “[u]ntil those weaknesses are fixed, financial and taxpayer data will remain unnecessarily vulnerable to inappropriate and undetected use, modification or disclosure.”

62. J. Russell George (“George”), the Treasury Inspector General for Tax Administration testified before the Senate Finance Committee (hereinafter “Hearing”) on June 2, 2015, and stated that the IRS had not addressed certain security weaknesses before the attack and failed to upgrade systems that would have deterred the organized security breach and subsequent tax fraud. At the hearing of the Senate Finance Committee, about one month after the breach, George told the panel that 44 of its recommendations to the IRS “have yet to be implemented.” Specifically, he said the IRS had not always applied high-risk computer security upgrades known as patches, and that the agency had failed to monitor many of its servers, “which put the IRS’ networks, data and applications at risk.”

63. Also, in response to a question from Hatch, George conceded that “[i]t would have been much more difficult if [the IRS] had implemented all of the recommendations we made.” George also stated “[w]e also found that the IRS was not monitoring a significant percentage of its [computer] servers, which puts data at risk,” and that the IRS needs “to be even more vigilant to protect the confidentiality of their data.”

64. Despite the IRS’s knowledge of its vulnerable and unsecure system, as well as data breach attempts on the IRS itself, along with the widely-publicized high-profile data breaches this past year, the IRS had many options which would have prevented the breach which include:

- A dynamic and aggressive security framework that would make it harder for fraudsters to impersonate legitimate taxpayers using information gleaned from around the Web;
- A more complex system that includes multi-factor authentication using biometrics and dynamic questions based on non-public information;
- Better use of a system the IRS already has in place: An easily hackable six-digit PIN that is available to taxpayers⁶;
- Or an authentication process that links phone numbers to taxpayers, similar to what online services such as Google now offer.

65. However, the IRS made an intentional decision not to implement the needed security measures without regard to the significant risk and danger to unsuspecting taxpayers. This decision by the IRS resulted in the loss of taxpayer data for Plaintiffs and the putative class.

PLAINTIFFS' DAMAGES

66. As a result of Defendants' willful, intentional disregard of Plaintiffs' and Class members' privacy rights, and the Defendants' failure to implement TIGTA's detailed recommendations and instructions to prevent the breach, Plaintiffs and Class Members have suffered and will continue to suffer damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress. They have suffered or are at increased risk of suffering from:

- the loss of the opportunity to control how their PII is used;
- the diminution in the value and/or use of their PII, entrusted to the IRS for the purpose of filing their annual income tax returns with the understanding that the IRS and its employees/managers would safeguard their PII against theft and not allow access and misuse of their PII by others;

6

- the compromise, publication and/or theft of their PII and the PII of their family members/spouses/dependents;
- out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
- lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the IRS breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse;
- costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets;
- unauthorized use of compromised PII to open new financial and/or health care or medical accounts;
- the continued risk to their PII, and the PII of their family members/spouses/dependents, which remains in the IRS's possession and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PII in their possession;
- current and 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 IRS breach for the remainder of the lives of the Class members and their families/spouses/dependents.

PLAINTIFFS' EXPERIENCES

A. Plaintiff Wendy Windrich's Experience

67. Wendy Windrich has never used or accessed the "Get Transcript" application.

68. In early June 2015, Plaintiff Windrich received a letter from the IRS stating that her and her husband's e-filing had been processed and their \$9,300 return had been electronically deposited into the account they provided in their e-filing.

69. This letter from the IRS alerted Plaintiff Windrich that something was wrong. Through their accountant, she had filed for an extension in late March or early April, and had not sent in money with the extension request. Further, Plaintiff Windrich has not received a refund from the IRS in many years and instead, she and her husband have had to write the IRS a check year after year.

70. After being alerted of possible fraud by the IRS return letter, Plaintiff Windrich informed the IRS and the IRS told her that the fraudulent tax return had very specific and personal information that had to be taken from her prior two years' income tax returns. Neither Plaintiff Windrich nor her husband had their personal information stolen or breached prior to the Get Transcript incident and the information supplied in the fraudulent tax return could only have come from the Get Transcript application. Based on information and belief, Plaintiff Windrich believes that her fraudulent tax return was filed with her family's personal information stolen from the Get Transcript application. During the phone call, the IRS instructed Plaintiff Windrich to go to the IRS website for instructions on how to report the potential fraud or suspicious activity.

71. The IRS then told Plaintiff Windrich that she would be given a special PIN number to include in her paper filing this year and that she would not be able to e-file for the foreseeable future. Plaintiff Windrich and her husband are IT professionals who have always taken great pride and effort in keeping their own computers secure, locked down, and free of viruses. Plaintiff Windrich is reasonably concerned about her and her husband's future, as well as their grown children's, as the family's PII was in the stolen tax data. The stolen information also includes their names, residential address, dates of

birth, telephone numbers, bank account information, and other personal information. Now the entire family's PII lie in the hands of the fraudsters.

72. Because the IRS required that she provide this highly important personal data to the IRS, under penalty of law if she were to refuse to do so, Plaintiff Windrich had a reasonable expectation that Defendants would have in place reasonable and appropriate security measures to ensure that her and her husband's, and their children's, personal data were secure.

73. Plaintiff Windrich and/or her husband have spent more than 30 hours dealing with the ramifications of this fraud. Further, because of this fraud, Plaintiff Windrich is no longer eligible for electronic filing of her tax returns for the "foreseeable future." Plaintiff Windrich reasonably believes that her PII was compromised and obtained by the cybercriminals through the IRS systems. Further, because the IRS permitted fraudsters' access to her account information by its knowing and willful implementation of the insecure Get Transcript application, Plaintiff Windrich is at a heightened risk of further identity theft requiring her to pay indefinitely for on-going credit monitoring.

B. Plaintiff Becky Welborn's Experience

74. Plaintiff Becky Welborn has never electronically filed her income tax returns.

75. Plaintiff Welborn self-filed her annual income taxes on April 15, 2015, in paper form. Five weeks after filing, Plaintiff Welborn began calling and checking the IRS website to inquire about her refund. The IRS website indicated that her return was being processed. When Plaintiff Welborn telephoned the IRS, the automated system took her through all of the standard questions and, like the website, stated that her return was being processed. The system then automatically disconnected the call.

76. After ten weeks of no refund, Plaintiff Welborn called the IRS automated telephone system and tried every option until she got a live person on the line. After two hours on the phone with

an IRS representative, the IRS representative explained to Plaintiff Welborn that someone had filed a duplicate joint return using her and her husband's social security numbers. The representative would not release any further information, but said that the fraudulent party had requested a transcript of Plaintiff Welborn's taxes through the Get Transcript application.

77. When Plaintiff Welborn inquired as to why the IRS did not notify Plaintiff about the fraudulent access to her income tax transcript, the agent responded that the IRS has not, but will be, sending a notification letter to notify the victims of the breach. Plaintiff Welborn asked if the IRS was taking any responsibility for the theft and the representative just referred Plaintiff Welborn to the IRS website.

78. Plaintiff Welborn is reasonably concerned about her and her husband's future, as well as their three children's, as the family's PII was in their stolen tax data. Now the entire family's PII lie in the hands of the fraudsters.

79. Because the IRS required that she provide this highly important personal data to the IRS, under penalty of law if she were to refuse to do so, Plaintiff Welborn had a reasonable expectation that Defendants would have in place reasonable and appropriate security measures to insure that her and her husband's, and their children's, personal data were secure.

80. Plaintiff Welborn and/or her husband have spent dozens of hours dealing with the ramifications of this fraud. Plaintiff Welborn had to change all of their bank account numbers, file a police report, place fraud alerts with all three credit agencies, file a report with the Federal Trade Commission, submit a fraud affidavit to the IRS, and request written copies of her family's credit reports from the three credit agencies. To date, Plaintiff Welborn has not received any written notification of the breach from the IRS. Further, because of this fraud, Plaintiff Welborn is no longer

eligible for electronic filing of her tax returns. The result is that any future potential tax refunds will be delayed for a significant period of time.

81. Further, because the IRS permitted fraudsters' access to her account information by its knowing and willful implementation of the insecure Get Transcript application, Plaintiff Welborn is at a heightened risk of further identity theft requiring her to pay indefinitely for on-going credit monitoring.

CLASS ACTION ALLEGATIONS

82. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of a class of similarly situated persons, which they initially propose be defined as follows:

All Tax filers of the United States and their spouses and/or dependants whose PII was compromised as a result of the "Get Transcript" application data breach.

83. Excluded from the proposed class are the IRS, Commissioner Koskinen, as well as agents, officers and directors (and their immediate family) of the IRS, their, and their affiliates and controlled persons. Also excluded is any judicial officer assigned to this case.

84. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4).

85. Numerosity—Fed. R. Civ. P. 23(a)(1). The members of the class are so numerous that joinder of all members is impracticable. While the exact number of class members is unknown to Plaintiffs at the present time and can only be ascertained through appropriate discovery, Plaintiffs believe that there are 500,000 or more members of the class located throughout the United States. It would be impracticable to join the class members individually.

86. Existence and predominance of common questions of law—Fed. R. Civ. P. 23(a)(2), 23(b)(3). Common questions of law and fact exist as to all members of the class and predominate over any questions solely affecting individual members of the class.

87. Among the many questions of law and fact common to the class are:

- whether Defendants' conduct violated the Privacy Act of 1974;
- whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to the security and integrity of these records;
- whether Defendants disclosed Plaintiffs' and Class members' PII without their prior written consent;
- whether Defendants' conduct was willful or with flagrant disregard for the security of Plaintiffs' and Class Members' PII;
- whether Defendants had a legal duty to use reasonable cyber security measures to protect Plaintiffs and Class members' PII;
- whether Defendants breached their legal duty by failing to protect Plaintiffs' and Class members' PII;
- whether Defendants acted willfully in failing to secure Plaintiffs' and Class members' PII;
- whether Plaintiffs and Class members are entitled to damages, declaratory or injunctive relief.

88. Typicality—Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of the claims of the members of the class. Among other things, Plaintiffs and Class members are all former, current, and prospective American income tax filers and their spouses and/or dependents who provided personal information in connection with the filing of their federal income tax returns and other sensitive documentation filed with the IRS.

89. Adequacy—Fed. R. Civ. P. 23(a)(4). Plaintiffs will adequately represent the proposed Class members. They have retained counsel competent and experienced in class action and internet privacy litigation and intend to pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of class members.

90. Superiority—Fed. R. Civ. P. 23(b)(3). A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiffs know of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action.

91. In the alternative, the class may be certified under Rule 23(b)(1), 23(b)(2) or 23(c)(4) because:

- the prosecution of separate actions by the individual members of the class would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants;
- the prosecution of separate actions by individual Class members would create a risk of adjudications that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests;
- Defendants acted or refused to act on grounds generally applicable to the class, thereby making appropriate final injunctive relief with respect to the members of the class as a whole; and
- the claims of class members are comprised of common issues that are appropriate for certification under Rule 23(c)(4).

CAUSES OF ACTION

COUNT ONE

(On behalf of Plaintiffs and Class Members against the IRS)

**VIOLATION OF PRIVACY ACT OF 1974, 5 U.S.C. § 552a
("PRIVACY ACT")**

92. Plaintiffs incorporate each and every allegation above as if fully set forth herein.

93. The IRS is an "agency" within the meaning of the Privacy Act.

94. Pursuant to 5 U.S.C. § 552a(b), agencies are prohibited from disclosing "any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains"

95. Pursuant to 5 U.S.C. § 552a(e)(10), "[e]ach agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

96. The IRS obtained and preserved Plaintiffs and Class members' PII, including tax return transcripts, and other records, in a system of records during the tax collection and assessment process.

97. The IRS is therefore prohibited from disclosing federal taxpayers' PII, under 5 U.S.C. § 552a(b), and is responsible for establishing appropriate "safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity," under 5 U.S.C. § 552a(e)(10).

98. The IRS is, and at all relevant times hereto was, required by law to comply with both FISMA and the Modernization Act. The IRS is also responsible for ensuring that its cyber security

systems comply with 5 U.S.C. § 552a and other rules and regulations governing cyber security practices.

99. However, as related herein, the IRS intentionally and willfully failed to comply with FISMA and the Modernization Act and 5 U.S.C. § 552a and other rules and regulations governing cyber security practices.

100. The IRS's history of non-compliance with FISMA's legal requirements that culminated in the IRS's risk-based decisions to make exceptions to its own policies and requirements in its decision not to follow TIGTA's 2014 instruction to take corrective actions for a more secure and less vulnerable security system, resulted in (1) the disclosure of Plaintiffs' and Class members' records without prior written consent in violation of 5 U.S.C. § 552a(b) and, ultimately, (2) the "substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members," that 5 U.S.C. § 552a(e)(10) is designed to protect against.

101. As a result of Defendants' intentional and willful conduct, Plaintiffs and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the Privacy Act. Such damages have included or may include without limitation: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to the IRS for the purpose of filing income tax returns and with the understanding that the IRS would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the IRS breach, including but not limited to efforts spent researching how to prevent,

detect, contest and recover from PII misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial accounts or file fraudulent tax returns; (8) the continued risk to their PII, and the PII of their family members, which remains in the IRS's possession and is subject to further breaches so long as the IRS fails to undertake appropriate and adequate measures to protect the PII in its possession; and (9) 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 IRS Breach for the remainder of the lives of the Plaintiffs, Class members, and their families. Plaintiffs and Class members are thus entitled to relief, pursuant to 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

COUNT TWO

(On behalf of Plaintiffs and Class members against the Defendants)

**VIOLATION OF THE ADMINISTRATIVE PROCEDURE ACT,
5 U.S.C. § 701, ET SEQ.**

102. Plaintiffs incorporate each and every allegation as if fully set forth herein.

103. The IRS was required to comply with FISMA and has a continuing obligation to comply with the Modernization Act. Moreover, under FISMA, Defendant Koskinen was required to exercise oversight of the IRS's information security policies and practices, including implementation of rules and standards complying with 40 U.S.C. § 11331. However, as is alleged above and incorporated herein, from 2010 to 2014, through a continuous course of conduct, the IRS intentionally failed to comply with FISMA and 40 U.S.C. § 11331 resulting in violations of the Privacy Act, 5 U.S.C. § 552a.

104. The IRS Defendants' non-compliance with FISMA's requirements was consistent from 2010 to 2014 and was not a valid exercise of discretion. FISMA and the Modernization Act are the law and, pursuant to FISMA's terms, Defendant Koskinen is required to oversee the IRS's compliance with

both. TIGTA found that he failed to do so and that his failure put the IRS's networks, data, and applications at risk. Ultimately the IRS's noncompliance with FISMA and the Modernization Act resulted in the Privacy Act violations at the center of this lawsuit.

105. The IRS's noncompliance with FISMA is well documented in each of TIGTA's annual audit reports issued from 2010 to 2014. As is alleged in the preceding paragraphs, in each of TIGTA's audit reports, the TIGTA instructed the IRS to bring its cybersecurity systems into compliance with FISMA, but each year, the IRS Defendants made the decision not to do so. For example, from 2012 to 2014, TIGTA told the IRS it was not in compliance with FISMA because of its failure to meet the level of performance specified by the Office of Management and Budget and Department of Homeland Security in the areas of (1) Identity and Access Management, and (2) Configuration Management. Nevertheless, the IRS Defendants repeatedly and intentionally made the decision not to comply with FISMA's requirements.

106. The IRS's continuous string of decisions not to comply with FISMA culminated in Koskinen's choice to launch the "Get Transcript" application despite knowing the major security vulnerabilities and the IRS's own declaration that its Information Security program was a "significant deficiency" from a financial reporting standpoint. This means weaknesses in its internal control environment were important enough to merit the attention of those charged with IRS governance.

107. The IRS Defendants' many decisions not to comply with FISMA including but not limited to (1) deciding not to implement 44 recommendations that would have protected taxpayer data and improved its overall security posture and, instead, (2) deciding to launch the "Get Transcript" application despite its chronic failure to meet the level of performance specified by the OMB and the Department of Homeland Security, constitute final agency actions because the decisions were the consummation of the IRS's decision making process, were not merely tentative or interlocutory nature,

and denied Plaintiffs and Class members the right to protection of their PII. Because the IRS Defendants' willful, intentional, and continuous course of conduct resulted in the IRS Breach in which Plaintiffs and Class members' PII was compromised, the IRS Defendants continuous string of decisions not to comply with FISMA caused violations of the Privacy Act and damages to Plaintiffs and Class members.

108. The IRS Defendants violated their obligation to comply with FISMA, 40 U.S.C. § 11331, and the Privacy Act because, for years, they ignored TIGTA's detailed instructions, and ultimately, decided to reject 44 of TIGTA's security recommendations.

109. Defendants' continuous string of decisions not to comply with FISMA—including TIGTA's recommendations of the IRS's Information Security program, was arbitrary, capricious and otherwise not in accordance with law; was in excess of statutory jurisdiction, authority, or limitations, or short of statutory right; and was without observance of procedure required by law.

110. Because of the IRS Defendants' decisions not to comply with FISMA, the IRS Defendants violated the Privacy Act, and Plaintiffs and Class members suffered a legal wrong, and were adversely affected insofar as cyber attackers gained access to their sensitive, confidential, and personal information.

111. Plaintiffs and Class members are thus entitled to declaratory and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

(a) Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' counsel to represent the class;

(b) Award Plaintiffs and Class members appropriate relief, including actual and statutory damages;

- (c) Award equitable, injunctive, and declaratory relief as may be appropriate;
- (d) Award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;
- (e) Award pre-judgment and post-judgment interest as prescribed by law; and,
- (f) Grant further and additional relief as this court may deem just and proper.


JURY TRIAL DEMANDED

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

Dated: August 20, 2015

Respectfully submitted,

ABBOTT LAW GROUP P.A.

By: 
Steven W. Teppler (DC Bar No. 445259)
E-mail: steppler@abbottlawpa.com

ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Ph: (904) 292-1111 / Fax: (904) 292-1220

Richard D. McCune (CA Bar. No. 132124)*
E-mail: rdm@mccunewright.com
David C. Wright (CA Bar No. 177468)*
E-Mail: dcw@mccunewright.com
Michele M. Vercoski (CA Bar No. 244010)*
E-mail: mmv@mccunewright.com

MCCUNE WRIGHT LLP
2068 Orange Tree Lane, Suite 216
Redlands, California 92374
Ph: (909) 557-1250 / Fax: (909) 557-1275

John A. Yanchunis (FL Bar No. 324681)*
E-mail: JYanchunis@ForThePeople.com
Patrick A. Barthle II (FL Bar No. 99286)*
E-mail: PBarthle@ForThePeople.com

MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida, 33602
Telephone: (813) 223-5505
Fax: (813) 222-4738

Joel R. Rhine (NC State Bar No. 16028)*

E-Mail: jrr@rhinelawfirm.com

RHINE LAW FIRM, P.C.

1612 Military Cutoff Road, Ste. 300

Wilmington, NC 28403

Telephone: (910) 777-7651

Fax: (910) 772-9062

**Pro Hac Vice Applications to be submitted*

Attorneys for Plaintiffs and Putative Class