

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO**

JACQUELINE LEWIS-GRIFFIN, Individually and On behalf of all others similarly situated, <p style="text-align: right;">Plaintiff,</p>)	Civil Action No.:
)	
)	JUDGE:
)	
v.)	CLASS ACTION COMPLAINT
)	
RBS WORLDPAY, INC.)	(JURY TRIAL DEMANDED)
)	
Defendant.)	

**CLASS ACTION COMPLAINT
WITH INJUNCTIVE RELIEF SOUGHT AND DEMAND FOR JURY TRIAL**

Plaintiff Jacqueline Lewis-Griffin ("Plaintiff") hereby brings this class action suit against RBS WorldPay, Inc. individually and on behalf of all others similarly situated, and hereby alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this suit on her own behalf and on behalf of all other persons or entities in the United States whose personal or financial data was stolen or compromised from RBS's computer system ("Plaintiffs" or the "Class").

INTRODUCTION

2. Plaintiffs bring this action as a class action pursuant to Rules 23(a), (b)(1), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure on behalf of all persons throughout the nation whose private financial information was negligently, deliberately, and/or recklessly allowed to be stolen from RBS WorldPay, Inc. ("RBS" or "Defendant"), in violation of the Fair Credit

Reporting Act, 15 U.S.C. § 1681 et seq. (“FCRA”), Ohio Rev. Code §1345.01 *et seq.*, and in violation of other statutory and common law causes of action. Defendant negligently, deliberately, and/or recklessly did not maintain reasonable procedures designed to limit the furnishing of this private financial information for the permissible purposes outlined under FCRA. As a result of Defendant’s negligent, deliberate, and/or reckless violations of FCRA, Plaintiff’s and Class members’ Consumer Reports were stolen without the consent of Plaintiff and Class members, and for no permissible purpose under FCRA.

3. Defendant’s actions constitute violations of FCRA, Ohio Rev. Code § 1345.01 *et seq.*, as well as common law negligence and breach of contract.

4. Plaintiff seeks damages suffered as a result of Defendant’s practices, including but not limited to statutory damages, compensatory damages, and injunctive relief.

PARTIES AND JURISDICTION

5. Plaintiff Jacqueline Lewis-Griffin resides at 4025 Wilmington Road, South Euclid, Ohio 44121 (Cuyahoga County). Plaintiff received a letter from RBS dated December 29, 2008 informing her that her personal and financial information is at risk from an intrusion into RBS’s computer system.

6. Defendant RBS WorldPay, Inc., is incorporated in Georgia. Its headquarters are at 600 Morgan Falls Rd., Atlanta, GA 30350. RBS is the “U.S. payment processing division of the Royal Bank of Scotland Group PLC.”, and is a “non-bank subsidiary of Citizens Financial Group.”¹ RBS can be served through its registered agent for service of process, The Prentice-Hall Corporation System, Inc., located at 50 West Broad Street, Suite 1800 in Columbus, Ohio 43215.

¹ See http://www.rbsworldpay.us/media/news_media25.htm.

7. At all times relevant to this complaint, RBS transacted business throughout the State of Ohio.

8. The Court has jurisdiction over the federal claims herein pursuant to 28 U.S.C. § 1331. The Court has supplemental jurisdiction over the state law claims herein under 28 U.S.C. § 1367. Further, the Court also has subject matter jurisdiction over this nationwide class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds \$5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). The Court has personal jurisdiction over Defendant because it owns and operates a business that conducts substantial business throughout Ohio.

9. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the acts giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

10. RBS describes itself as a "provider of electronic payment processing services- including credit, debit, EBT, checks, gift cards, e-commerce, customer loyalty cards, fleet cards, prepaid cards, ATM processing and cash management services."²

11. On December 29, 2008, RBS mailed letters to individuals affected by the data breach stating:

RBS WorldPay recently learned about a situation involving prepaid gift, rewards and payroll cards for which RBS WorldPay is the service provider. We are investigating fraudulent activity as a result of unauthorized access to our system. Information such as name, address, telephone number, Social Security number, card account number, PIN, and financial account information may have been inappropriately accessed by an unauthorized person.³

² *See* http://www.rbsworldpay.us/media/news_media25.htm.

³ *See* http://www.rbsworldpay.us/RBS_WorldPay_Substitute_Website_Notice_Dec_23.pdf.

12. Also, on December 23, 2008, RBS issued a press release stating:

RBS WorldPay (formerly RBS Lynk), the U.S. payment processing arm of The Royal Bank of Scotland Group, today announced that its computer system had been improperly accessed by an unauthorized party.

The affected pre-paid cards include payroll cards and open-loop gift cards. Personal information associated with certain payroll cards may have been improperly accessed....

The fraud that has been identified to-date is associated with RBS WorldPay's computer system supporting its U.S. pre-paid and open-loop gift card issuing business. Actual fraud has been committed on approximately 100 cards... Certain personal information of approximately 1.5 million cardholders and other individuals may have been affected and, of this group, Social Security numbers of 1.1 million people may have been accessed.⁴

13. The approximately 100 cards that experienced actual fraud were "payroll cards."⁵

14. According to RBS, payroll cards are used to pay wages to employees. A payroll card is a reloadable card that can be used at any point of sale location that accepts credit and debit cards. Cardholders are generally able to make the same transactions available to them with a debit card, including ATM withdrawals, point of purchases, and bill payment. Payroll cards are reloadable with funds loaded onto the cards directly by the cardholder's employer. RBS issues and processes payroll card programs.⁶

15. According to RBS, "open-loop gift cards" are available from a wide range of retailers. The vast majority are sold in denomination of \$25.00 - \$200.00. Retailers hold stocks of these gift cards, and the cards are activated upon purchase. Open-loop gift cards can be used at any retailer that accepts credit and debit cards, not just the retailer from which the card was

⁴ See http://www.rbsworldpay.us/RBS_WorldPay_Press_Release_Dec_23.pdf.

⁵ See http://www.rbsworldpay.us/prepaid_info.html.

⁶ See http://www.rbsworldpay.us/RBS_WorldPay_Payroll_Fact_Sheet_Dec_23.pdf.

purchased. RBS provides approximately 10 million gift cards annually to retailers across the U.S.⁷

16. Class members are at risk of fraud and identity theft stemming from the data breach. Class members who held gift cards and payroll cards are at risk of, *inter alia*, fraudulent charges being incurred on those cards. Class members whose Social Security numbers and related information have been compromised are at risk of, *inter alia*, fraudulent accounts being opened in their name.

17. Class members have and will continue to experience considerable risk and inconvenience from this breach. TBS encouraged Class members to: (i) obtain credit reports from credit reporting agencies; (ii) “carefully review your credit reports and bank, credit card, payment card and other account statements” for the next “12 to 24 months”; (iii) “look for accounts you did not open”; (iv) call local police and file an identity theft report if fraudulent activity occurs; (v) call consumer reporting agencies if fraud appears on credit reports; (vi) place a 90-day fraud alert on your credit file; and (vii) place a security freeze on your credit file.⁸ These steps may require out-of-pocket costs. For example, RBS disclosed that “consumer reporting agencies may charge a reasonable fee to place a freeze on your account.” *Id.* Also, although consumers are entitled to one free credit report per year from each of the three major credit reporting agencies (Equifax, Experian, and TransUnion), fees are imposed for additional credit reports. Further, Class members might purchase credit monitoring services to monitor their credit histories for fraud.

⁷ See http://www.rbsworldpay.us/RBS_WorldPay_Gift_Card_Fact_Sheet_Dec_23.pdf.

⁸ See http://www.rbsworldpay.us/RBS_WorldPay_Substitute_Website_Notice_Dec_23.pdf.

18. RBS stated that it is re-setting PINs for all PIN-enabled cards.⁹ This is an inconvenience to Class members, as they will lose access to funds while the PINs are being reset and while awaiting notification of the new PINs.

19. RBS is not canceling and re-issuing affected gift cards purchased and activated by consumers.¹⁰

20. RBS identified the data breach on November 10, 2008.¹¹ However, RBS waited approximately 43 days to publicly announce the breach, issuing a press release on December 23, 2008. Notably, RBS delayed announcing the breach until the end of the busy holiday shopping season, a period when heavy sales of gift cards occur.

21. RBS's Privacy Policy on its website stated:

- "Except for access to data by RBS WorldPay Personnel or the sponsor of your card program required to conduct business, you will be the only person accessing your data."
- "We use security techniques designed to protect our customer data...."
- "In keeping with our strong interest in consumer privacy protection, RBS WorldPay keeps abreast of current industry initiatives to preserve individual privacy rights on the Internet and in all aspects of electronic commerce."¹²

RBS violated these policies and failed to comply with the stated industry initiatives.

22. RBS was intimately familiar with industry-wide duties and standards regarding data security. Ironically, as part of its business, RBS offers data breach protection services to its merchant clients. RBS's services include: (i) assessing clients' risks and vulnerabilities of data breach; (ii) scanning clients' point-of-sale and computer networks to identify potential problems

⁹ See http://www.rbsworldpay.us/prepaid_info.html.

¹⁰ See http://www.rbsworldpay.us/RBS_WorldPay_Press_Release_Dec_23.pdf.

¹¹ See http://www.rbsworldpay.us/RBS_WorldPay_Press_Release_Dec_23.pdf.

¹² See <http://www.rbsworldpay.us/privacy.htm>.

regarding data security; and (iii) informing clients about Payment Card Industry (PCI) best practices.¹³ In light of this heightened knowledge, RBS knew or should have known it had security vulnerabilities.

23. RBS is a “merchant acquire bank,” which is describes as follows:

Merchant acquiring is the term used to describe the services provided by payment processing companies to enable merchants to accept their customers’ payment cards at point of sale. Merchant acquirers generally perform [several] key functions....Providing the means to authorize valid card transactions at client merchant locations; Facilitating the clearing and settlement of the transactions through the payment network;

...Card or merchant acquiring is the infrastructure that allows cardholders to use credit, debit or pre-paid cards at point of sale, (e.g. in a shop or restaurant or for an online purchase), and for the merchant to receive payment for that purchase.¹⁴

Merchant acquiring banks are required to comply with various data security standards, including but not limited to the Payment Card Industry (PCI) Data Security Standard. RBS’s data security environment failed despite these PCI requirements.

24. As a result of RBS’s conduct, Class members suffered damages including but not limited to:

a. out-of-pocket loss for, *inter alia*, fraudulent charges on their cards (to the extent not reversed by RBS), cost of credit monitoring and/or credit card monitoring services, costs of identity theft insurance, costs to obtain credit reports, costs for credit freezes, and unpaid time off from work responding to the breach;

b. loss of use of their cards while PIN numbers were re-issued and/or fraudulent charges were investigated by RBS;

¹³ See <http://www.rbsworldpay.us/products/databreach.htm>.

¹⁴ See http://www.rbsworldpay.us/RBS_WorldPay_Merchant_Aquiring_Fact_Sheet_Dec_23.pdf.

- c. fear and apprehension of fraud, loss of money, and identity theft;
- d. the burden of closely scrutinizing account statements and credit reports for fraud, formally disputing fraudulent activity, filing police reports, and placing fraud alerts and/or credit freezes on credit files; and
- e. other economic and non-economic damages.

25. The Class is also entitled to injunctive relief including but not limited to: (i) the provision of credit monitoring services and/or identity theft insurance; and (ii) the requirement that RBS enhance the security of its computer system to minimize the likelihood of intrusions in the future. Injunctive relief is required because money damages alone are insufficient to redress the irreparable harm that Class members face absent these injunctive measures.

26. RBS has offered one year of free credit monitoring services to certain affected individuals whose Social Security numbers are at risk.¹⁵ One year of coverage is inadequate. Class members need several years of protection because identity thieves often do not use the stolen data for lengthy periods of time, waiting for victims to become lax in monitoring their accounts. Also, Class members need identity theft insurance (commonly packaged with credit monitoring) in addition to credit monitoring.

CONSEQUENCES OF BREACH

27. As defined in the Fair and Accurate Credit Transactions Act of 2003, Pub. L 08-159, Dec. 4, 2003 (FACTA) “identity theft” is a fraud that is committed or attempted, using a person’s identifying information with authority. Generally, identity theft occurs when a person’s identifying information is used to commit fraud or other crimes. These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government fraud. The Federal Trade

¹⁵ See http://www.rbsworldpay.us/RBS_WorldPay_Substitute_Website_Notice_Dec_23.pdf.

Commission (“FTC”) has stated that identity theft has been a serious problem in recent years, with approximately 9 million Americans as the victims of identity theft each year.¹⁶

28. As the United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”), more than 570 breaches involving theft of personal identifiers such as social security numbers were reported by the news media from January 2005 through January 2006.¹⁷ As the GAO Report states, these data breaches involve the “unauthorized or unintentional exposure, disclosure, or loss of confidential personal information, which can include personally identifiable information such as Social Security numbers (SSN) or financial information such as credit card numbers.”

29. The GAO Report stated that identity thieves can use identifying data such as social security numbers to open financial accounts and incur charges and credit in a person’s name. As the GAO has stated, this type of identity theft is the “most damaging” because it may take some time for the victim to become aware of the theft and can cause significant harm to the victim’s credit rating.

30. In addition, the GAO states that victims of identity theft will face “substantial costs and inconvenience repairing damage to their credit records,” as well as the damage to their “good name.”

31. According to the Federal Trade Commission (FTC), nine million Americans have their identities stolen each year.¹⁸ Identity theft victims must spend countless hours and money repairing damage to their good name and credit record. Identity thieves use stolen personal information such as social security numbers for a variety of crimes, including credit card fraud,

¹⁶See, “About Identity Theft,” in FTC Publication, Fighting Back Against Identity Theft, available at <http://www.ftc.gov/bcp/edu/microsites/idtheft/comsu,ers/about-identity-theft.html>.

¹⁷See, <http://www.gao.gov/new.items/d07737.pdf>.

¹⁸See, FTC Identity Theft Site, <http://www.ftc.gov/bcp/edu/microsites/idtheft/comsu,ers/about-identity-theft.html>.

phone or utilities fraud, and bank/finance fraud. In addition, a person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office, which conducted a comprehensive and extensive study of 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.¹⁹

32. Identity theft crimes often include more than just crimes of financial loss. Identity thieves also commit various types of government fraud, such as: obtaining a driver's license or official identification card in the victim's name but with their picture; using the victim's name and social security number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or get medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.

33. The unauthorized disclosure of a person's social security number can be particularly damaging since social security numbers cannot be easily replaced like a credit card. In order to obtain a new social security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse.²⁰ Thus, a person whose personal information has been stolen cannot obtain a new social security number until the damage has already been done. Furthermore, obtaining a new social security number is not an absolute prevention against identity theft. Governmental agencies, private businesses, and credit

¹⁹ See, <http://www.gao.gov/new.items/d07737.pdf>.

²⁰ See, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327.

reporting businesses likely still have the person's records under the old number, and using a new number will not guarantee a fresh start. For some victims of identity theft a new number may actually create new problems. Because prior positive credit information is not associated with the new social security number, it is more difficult to obtain credit due to the absence of a credit history.

34. Thus, Plaintiffs and the Class Members now face years of constant surveillance, monitoring and loss of rights, not to determine whether they will become an identity theft victim, because they already are, but to prevent further loss and damage.

CLASS ACTION ALLEGATIONS

35. This action is brought on behalf of Plaintiff, individually and as a class action, on behalf of all persons throughout the nation whose Personal Financial Information was negligently, willfully, and/or recklessly allowed to be stolen from the RBS as a result of the data breach ("the Class"). The Class does not include Defendant, or its officers, directors, agents, or employees

36. The Class is composed of millions of consumers, the joinder of which in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

37. The rights of each member of the Class were violated in a similar fashion based upon Defendant's uniform actions and inactions.

38. Questions of law and fact common to the Class predominate over questions which may affect individual Class members, including, *inter alia*:

- a. whether Defendant is a consumer reporting agency as defined by 15 U.S.C. § 1681a(f);

- b. whether Defendant violated FCRA by failing to properly maintain reasonable procedures designed to limit the furnishing of Consumer Reports to the permissible purposes outlined under FCRA;
- c. whether Defendant violated FCRA when it allowed third parties access to Plaintiff's and Class members' Personal Financial Information;
- d. whether Defendant's conduct was deliberate and/or reckless;
- e. whether Defendant's conduct was negligent;
- f. whether Defendant's conduct constitutes an unfair and/or deceptive trade practice;
- g. whether Defendant was negligent in collecting and storing the Personal Financial Information of consumers;
- h. whether Defendant took reasonable measures to safeguard consumers' Personal Financial Information;
- i. whether Defendant owed a duty to Plaintiff and other members of the Class to protect their Personal Financial Information;
- j. whether Defendant breached its duty to exercise reasonable care in storing Plaintiff's and other members of the Class' Personal Financial Information by storing that information on its computer systems and in its physical possession;
- k. whether Defendant breached a duty by failing to keep Plaintiff's and other members of the Class' Personal Financial Information secure;
- l. whether Defendant was negligent in failing to keep Plaintiff's and other members of the Class' Personal Financial Information secure;
- m. whether Plaintiff and other members of the Class have sustained damages, and if so, what is the proper measure of those damages;
- n. whether statutory damages are proper in this matter;
- o. whether injunctive relief is appropriate in this matter;
- p. whether Defendant failed to properly give notice pursuant to Ohio Rev. Code § 1349.19; and
- q. whether Defendant's conduct constitutes a violation of Ohio Rev. Code §1345.01 *et seq.*

39. Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no interest that is antagonistic to or that irreconcilably conflicts with those of other members of the Class.

40. Plaintiff has retained counsel competent and experienced in the prosecution of class action litigation.

41. A class action is superior to all other available methods for the fair and efficient adjudication of Plaintiff's and the Class members' claims. Plaintiff and the members of the Class have suffered irreparable harm as a result of Defendant's deceptive, intentional, reckless, negligent, and unlawful conduct. The damages suffered by individual Class members may be relatively small, and thus few, if any individual class members can afford to seek legal redress on an individual basis for the wrong complained of herein. Absent a class action, Plaintiff and members of the Class will continue to suffer losses as a result of Defendant's unlawful and negligent conduct.

FIRST CAUSE OF ACTION

**INTENTIONAL VIOLATIONS OF
THE FAIR CREDIT REPORTING ACT**

42. Plaintiff re-alleges paragraphs 1 through 41 as if fully set forth herein.

43. This is a claim for violation of the Fair Credit Reporting Act ("FCRA").

44. FCRA was created to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information." *See* 15 U.S.C. § 1681 *et seq.*

45. In compliance with FCRA, the FTC codified 16 CFR § 682 *et. seq.*, which regulates the responsibility of companies and individuals who possess Consumer Information. The purpose of the section was to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information. See 16 C.F.R. 682.2(a).

46. “Consumer information” is defined as “any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.” 16 C.F.R. § 682.1(b).

47. The Personal Financial Information stolen was Consumer Information pursuant to 16 C.F.R. § 682.1 and FCRA.

48. 16 C.F.R. § 682.3 requires that “[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.”

49. “Disposal” is defined as “the...transfer of any medium, including computer equipment, upon which consumer information is stored.”

50. Under FCRA, a “consumer report” means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or

insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under 15 U.S.C. § 1681b. *See* 15 U.S.C. § 1681a(d)(1).

51. Further, a “consumer reporting agency” means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports. 15 U.S.C. § 1681a(f).

52. Plaintiff and the other Class members are “consumers” or “persons,” as defined and construed under FCRA. *See* 15 U.S.C. §§ 1681a(b) & (c).

53. Defendants maintain Consumer Reports as defined under the FCRA, because they are written, oral, or other communications of any information which bear on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under section 15 U.S.C. § 1681b.

54. Defendant was required under FCRA to take reasonable measures to protect against unauthorized access while transferring the Consumer Information. *See* 16 C.F.R. § 682.3.

55. In conscious disregard for the rights of Plaintiff and the other members of the Class, Defendant willfully and/or recklessly did not maintain reasonable procedures designed to protect against unauthorized access while transferring the Personal Financial Information.

56. As enumerated above, Defendant's deliberate and/or reckless conduct allowed third-parties to steal, or otherwise access, the Personal Financial Information without Plaintiff's or other members of the Class' consent and for no permissible purpose under FCRA.

57. Defendant's conduct violated FCRA, and Plaintiff and other members of the Class have been damaged by Defendant's willful and/or reckless actions.

58. As a result of Defendant's conduct, Plaintiff and other members of the Class are entitled to actual damages sustained and statutory damages of not less than \$100 and not more than \$1,000, as well as the costs and attorney's fees in bringing this action. 15 U.S.C. § 1681n.

SECOND CAUSE OF ACTION

NEGLIGENT VIOLATIONS OF THE FAIR CREDIT REPORTING ACT

59. Plaintiff re-alleges paragraphs 1 through 58 as if fully set forth herein.

60. This is a claim for negligent violation of the Fair Credit Reporting Act ("FCRA").

61. FCRA requires the proper disposal or transfer of Consumer Information. *See* 15 USCA §1681w; 16 C.F.R. § 682 *et. seq.*

62. In compliance with FCRA, the FTC codified 16 CFR § 682 *et. seq.* which regulates the responsibility of companies and individuals who possess Consumer Information. The purpose of the FCRA was to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information." *See* 16 C.F.R. 682.2(a).

63. "Consumer information" is defined as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data." 16 C.F.R. § 682.1(b).

64. The Personal Financial Information stolen was Consumer Information pursuant to 16 C.F.R. § 682.1 and FCRA.

65. 16 C.F.R. § 682.3 requires that "[a]ny person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."

66. "Disposal" is defined as "the...transfer of any medium, including computer equipment, upon which consumer information is stored.

67. Under FCRA, a "consumer report" means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other purpose authorized under 15 U.S.C. § 1681b. *See* 15 U.S.C. § 1681a(d)(1).

68. Further, a "consumer reporting agency" means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the

practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports. 15 U.S.C. § 1681a(f).

69. Defendant is a consumer reporting agency and/or possesses and transfers information derived from a consumer report.

70. Plaintiff and the other members of the Class are “consumers” or “persons,” as defined and construed under FCRA. *See* 15 U.S.C. §§ 1681a(b) & (c).

71. Defendant was required under FCRA to take reasonable measures to protect against unauthorized access while transferring the Personal Financial Information. *See* 16 C.F.R. § 682.3.

72. Defendant was negligent in failing to maintain reasonable procedures designed protect against unauthorized access while transferring the Personal Financial Information.

73. As enumerated above, Defendant’s conduct allowed third-parties to steal, or otherwise access, the Personal Financial Information without Plaintiff’s or other members of the Class’ consent and for no permissible purpose under FCRA.

74. Defendants conduct violated FCRA, and Plaintiff and other members of the Class have been damaged by Defendant’s negligent actions.

75. As a result of Defendant’s conduct, Plaintiff is entitled to actual damages to be proven at trial, as well as the costs and attorney’s fees in bringing this action. 15 U.S.C. § 1681.

THIRD CAUSE OF ACTION

VIOLATIONS OF OHIO REV. CODE §1345.01 ET SEQ. **(for Ohio residents only)**

76. Plaintiff re-alleges paragraphs 1 through 75 as if fully set forth herein.

77. This is a claim for violation of Ohio Rev. Code §1345.01 *et seq.*

78. Ohio Rev. Code §1345.01 *et seq.* provides that unfair methods of competition, unconscionable acts and practices, and unfair or deceptive acts or practices in the conduct “of any trade or commerce” are unlawful.

79. Plaintiff and the other members of the Class are “persons” as defined and construed under Ohio Rev. Code §1345.01.

80. Defendant’s conduct as alleged herein occurred in the course of trade or commerce.

81. Defendant’s failure to maintain reasonable procedures designed to protect against unauthorized access while transferring the Personal Financial Information constitutes an unfair or deceptive trade practice.

82. Further, Defendant’s failure to properly give notice of the breach of the security of its computerized data system pursuant to Ohio Rev. Code §1345.01 *et seq.* constitutes an unfair or deceptive practice.

83. Plaintiff and other members of the Class suffered actual damages and ascertainable losses as a result of Defendant’s deceptive and/or unfair trade practices, including but not limited to: expenses for credit monitoring, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

FOURTH CAUSE OF ACTION

NEGLIGENCE

84. Plaintiff re-alleges paragraphs 1 through 83 as if fully set forth herein.

85. Defendant came into possession of Plaintiff's and other members of the Class' Personal Financial Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen.

86. Defendant had a duty to timely disclose the fact that Plaintiff's and other members of the Class' Personal Financial Information within its possession had been, or was reasonably believed to have been, compromised.

87. Defendant had a duty to protect Plaintiff's Personal Financial Information within its possession.

88. Defendant further had a duty to hire and supervise trustworthy employees as well as to have procedures in place to detect and prevent the theft or dissemination of Plaintiff's Personal Financial Information. This breach of security and unauthorized access was reasonably foreseeable to Defendant.

89. Defendant, through its acts and/or omissions, unlawfully breached its duty to Plaintiff and other members of the Class by failing to maintain reasonable procedures designed to protect against unauthorized access while transferring the Personal Financial Information within its possession.

90. Defendant, through its actions and/or omissions, breached its duty to timely disclose the fact that Plaintiff and other members of the Class' Personal Financial Information within its possession had been, or was reasonably believed to have been, compromised.

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

92. Plaintiff and other members of the Class' Personal Financial Information was compromised, viewed, and/or stolen as the proximate result of Defendant failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures to protect and safeguard the private, non-public, personal and financial information within its possession.

93. Plaintiff and other members of the Class suffered actual damages including, but not limited to: expenses for credit monitoring, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

FIFTH CAUSE OF ACTION

BREACH OF CONTRACT

94. Plaintiff re-alleges paragraphs 1 through 93 as if fully set forth herein.

95. Defendant came into possession of Plaintiff's and other members of the Class' Personal Financial Information due to its contracts with the various entities to provide credit card, debit card, and check processing in a secure manner. Defendant's contracts with the business entities were based upon its ability to protect such information. Plaintiff and other members of the Class, who patronize these business entities, are intended third-party beneficiaries of these contracts.

96. Defendant did not safeguard and protect Plaintiff's and other members of the Class' Personal Financial Information from being compromised and/or stolen. Indeed, Defendant allowed this information to be stolen.

97. Because Defendant allowed the disclosure of Plaintiff and other members of the Class' Personal Financial Information, and failed to safeguard and protect such information from

being compromised and/or stolen, Defendant breached its contract with the various business entities to which Plaintiff and other members of the Class are intended third party beneficiaries.

98. Plaintiff and other members of the Class suffered actual damages including, but not limited to: anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

SIXTH CAUSE OF ACTION

VIOLATION OF OHIO'S AND OTHER STATES' DATA BREACH NOTIFICATION LAWS O.R.C. § 1349.19

99. Plaintiff re-alleges paragraphs 1 through 98 as if fully set forth herein.

100. Ohio Rev. Code § 1349.19, along with various other state laws, require organizations to notify consumers whose personal information has been exposed in a data breach in a timely fashion.

101. Defendant came into possession of Plaintiff and other members of the Class' Personal Financial Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen.

102. Defendant had a duty to promptly disclose the fact that Plaintiff and other members of the Class' Personal Financial Information within its possession had been, or was reasonably believed to have been, compromised.

103. Defendant, through its actions and/or omissions, failed to timely disclose the fact that Plaintiff's and the other members of the Class' Personal Financial Information within its possession had been, or was reasonably believed to have been, compromised.

104. Defendant's failure to timely give notice of the breach of the security of its computerized data system violates Ohio law and various other states' data breach notification laws.

105. Plaintiff and the other members of the Class request that an injunction be issued to require Defendant to promptly provide notice to those individuals whose Personal Financial Information has been compromised.

SEVENTH CAUSE OF ACTION

NEGLIGENCE PER SE

106. Plaintiff re-alleges paragraphs 1 through 105 as if fully set forth herein.

107. In addition to the FCRA and Ohio Rev. Code § 1349.19, the GLBA (15 USC §6801) provides:

(a) Privacy obligation policy

It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) Financial institutions safeguards

In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards -

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

108. Defendants' conduct constitutes a violation their regulatory and statutory duties, including, but not limited to, violations of the FCRA and the GLBA.

109. Defendants' violation of these regulatory and statutory duties constitutes negligence per se.

110. As a direct and proximate result of the Defendants' negligence per se, the Plaintiffs and the Class Members have suffered harm and damages, the full extent of which will be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, respectfully ask that the Court enter an Order:

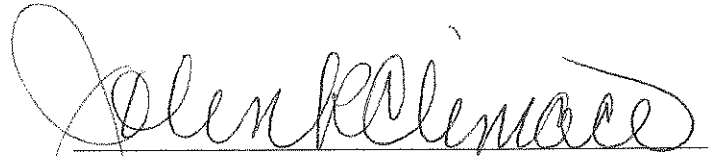
- (a) certifying this matter as a class action with Plaintiff as Class Representative and designating Plaintiff's counsel as Class Counsel;
- (b) finding that Defendant willfully and/or recklessly violated FCRA due to its failure to maintain reasonable procedures designed protect against unauthorized access while transferring the Personal Financial Information;
- (c) finding that Defendant negligently violated the FCRA due to its failure to maintain reasonable procedures designed to protect against unauthorized access while transferring the Personal Financial Information;
- (d) declaring that Defendant's failure to maintain reasonable procedures designed TO protect against unauthorized access while transferring the Personal Financial Information constitutes an unfair or deceptive trade practice and enjoining such conduct;
- (e) declaring that Defendants' failure to properly give notice of the breach of the security of its computerized data system pursuant to Ohio R.C. § 1349.19, and all similar data breach notification statutes constitutes an unfair or deceptive practice and entering an injunction to remedy such failure;

- (f) finding that Defendant breached its contract to safeguard and protect Plaintiff and the Class' Personal Financial Information stored on its computer systems and in its physical possession;
- (g) finding that Defendant was negligent in protecting Plaintiff and the Class' Personal Financial Information in its physical possession;
- (h) requiring Defendant to pay for monitoring Plaintiff's and other members of the Class' financial accounts as well as to compensate Plaintiff and other members of the Class for all damages that result from the unauthorized release of their private information;
- (i) enjoining Defendant from actions which place consumers at a risk of future security breaches;
- (j) requiring Defendant to pay actual damages sustained and/or statutory damages of not less than \$100 and not more than \$1,000;
- (k) awarding actual and/or compensatory damages as provided by Ohio Rev. Code §1345.01 *et seq.*;
- (l) awarding the costs of this proceeding and attorneys' fees, as provided by Ohio Rev. Code §1345.01 *et seq.*;
- (m) awarding damages to Plaintiff and the Class under the common law theories alleged;
- (n) requiring Defendant to pay Plaintiff and the Class' reasonable attorneys' fees and costs of litigation;
- (o) requiring Defendant to make Plaintiff and other members of the Class whole;
- (p) requiring Defendant to pay treble damages; and
- (q) providing for such other legal and/or equitable relief as justice requires.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, demand a trial by jury on all issues so triable.

DATED: February 5th, 2009



JOHN R. CLIMACO (#0011456)
DAVID M. CUPPAGE (#0047104)
SCOTT D. SIMPKINS (#0066775)
**CLIMACO, LEFKOWITZ, PECA,
WILCOX & GAROFOLI CO., L.P.A.**

55 Public Square, Suite 1950
Cleveland, OH 44113
Telephone: 216/621-8484
216/771-1632 (fax)
jrcлим@climacolaw.com
sdsimp@climacolaw.com
dmcupp@climacolaw.com

FRANK E. PISCITELLI, JR. (#0062128)
FRANK PISCITELLI CO., LPA
55 Public Square, Suite 1950
Cleveland, OH 44113
Telephone: 216/931-7000
216/931-9925 (fax)
frank@piscitellilaw.com

D. SCOTT KALISH (#0063002)
SCOTT KALISH CO., L.L.C.
1468 West 9th Street, Suite 405
Cleveland, OH 44113
Telephone: 216/502-0570
scottkalishcollc@cs.com