

JAN 06 2009

JAMES N. HATTEN, Clerk
By:  Deputy Clerk

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

KEITH IRWIN, on behalf of himself)
and all others similarly situated,)
)
Plaintiff,)
)
v.)
)
RBS WORLDPAY, INC.,)
)
)
Defendant.)

Civ. Action No. **1 09-CV-0033**

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Keith Irwin ("Plaintiff") hereby brings this class action suit against RBS WorldPay, Inc. ("RBS," the "Company," or "Defendant"). Plaintiff makes the following allegations based upon an investigation undertaken by Plaintiff's counsel, which included, *inter alia*, review and analysis of RBS's website, various news articles, and third party websites.

NATURE OF THE ACTION

1. Plaintiff brings this suit on his 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").

2. This suit seeks to redress RBS's failure to adequately safeguard Plaintiffs' private personal and financial information from an unauthorized individual. Compromised information includes names, addresses, telephone numbers, Social Security numbers, card account numbers, PINs, and financial account information. According to RBS, approximately 1.5 million individuals may have been affected by the breach. Actual fraud has occurred on at least 100 occasions.

JURISDICTION AND VENUE

3. Jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1332(d)(2), diversity, as the matter in controversy exceeds \$5 million, at least one class member has diverse citizenship from Defendant, and there are more than 100 class members.

4. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a)(2) because this is the judicial district in which a substantial part of the events giving rise to the claims occurred.

PARTIES

5. Plaintiff Keith Irwin resides in Pennsylvania. Plaintiff received a letter from RBS WorldPay dated December 23, 2008 informing him that his 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 WorldPay, Inc. can be served through its registered agent for service of process, Corporation Service Company, located at 40 Technology Parkway, #3, Norcross, Gwinnett County, Georgia 30092.

OPERATIVE FACTS

7. 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

8. On December 23, 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

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

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

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

9. 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

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

11. 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 sale purchases, online purchases, and bill payment. Payroll cards are reloadable

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

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

with funds loaded onto the cards directly by the cardholder's employer. RBS issues and processes payroll card programs.⁶

12. According to RBS, "open-loop gift cards" are available from a wide range of retailers. The vast majority are sold in denominations of \$25-\$200. 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 purchased. RBS provides approximately 10 million gift cards annually to retailers across the U.S.⁷

13. 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.

14. Class members have and will continue to experience considerable risk and inconvenience from this breach. RBS 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

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

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

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.

15. 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.

16. RBS is not cancelling and re-issuing affected gift cards purchased and activated by consumers.¹⁰ Thus, consumers face a continuing risk of fraud on their cards.

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

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

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

17. 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.

18. 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.

19. 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 a data breach; (ii) scanning clients' point-of-sale and computer networks to identify potential problems regarding data security; and

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

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

(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.

20. RBS is a “merchant acquiring 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.

21. 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

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

¹⁴ See http://www.rbsworldpay.us/RBS_WorldPay_Merchant_Acquiring_Fact_Sheet_Dec_23.pdf

(to the extent not reversed by RBS), costs 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;

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.

22. 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.

23. 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.

CLASS ACTION ALLEGATIONS

24. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of himself and all others similarly situated (the “Class”), defined as follows:

All persons or entities in the United States whose personal or financial data was stolen or compromised from RBS WorldPay Inc.’s computer system.

Excluded from the Class are RBS and its officers and directors.

25. The Class is so numerous that joinder of all Class members is impracticable. RBS disclosed that “personal information of approximately 1.5 million cardholders and other individuals may have been affected and, of this group,

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

Social Security numbers of 1.1 million people may have been accessed.”¹⁶

26. RBS’s conduct in failing to: (i) safeguard Class members’ personal and financial data, and (ii) timely notify Class members of the security breach as soon as practical after the breach was discovered is uniform among the Class.

27. Questions of law and fact common to all Class members predominate over any questions affecting only individual members. Questions of law and fact common to the Class include:

- a. whether RBS breached a duty in failing to safeguard Class members’ financial and personal data;
- b. whether RBS violated industry standards regarding the safeguarding of Class members’ financial and personal data;
- c. whether RBS failed to timely notify Class members of the security breach as soon as practical after the breach was discovered;
- d. whether RBS breached implied contracts by failing to safeguard Class members’ financial and personal data;
- e. whether RBS engaged in deceptive business practices by failing to safeguard Class members’ financial and personal data; and
- f. whether Plaintiff and the Class have been damaged from RBS’s

¹⁶ See http://www.rbsworldpay.us/RBS_WorldPay_Press_Release_Dec_23.pdf.

conduct.

28. Plaintiff's claims as described herein are typical of the claims of all Class members. The claims of Plaintiff and the Class arise from the same set of facts regarding RBS's failure to protect personal and financial data. Plaintiff maintains no interests that are antagonistic to the interests of other Class members.

29. Plaintiff is committed to the vigorous prosecution of this action and has retained competent counsel experienced in prosecuting class actions of this type. Plaintiff is an adequate representative of the Class and will fairly and adequately protect the interests of the Class.

30. A class action is a fair and efficient method of adjudicating the claims of Plaintiff and the Class for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class member;

b. Litigating separate non-class actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class. This would establish incompatible standards of conduct for RBS or allow some Class members' claims to adversely affect other Class members' ability to protect their interests;

c. Plaintiff anticipates no difficulty in the management of this litigation as a class action;

d. the Class is readily definable; and

e. prosecution as a class action will eliminate the possibility of repetitious litigation while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

31. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

COUNT I: NEGLIGENCE

32. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

33. RBS assumed a duty, and had duties imposed by industry standards, to use reasonable care to keep Class members' personal and financial information private and secure. By its acts and omissions described herein, RBS unlawfully breached its duties. The Class was damaged thereby.

34. 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.

35. The compromise of Class members' personal and financial information, and the resulting out of pocket loss, burden, fear, anxiety, emotional distress, loss of time spent seeking to prevent or undo harm, and other economic and non-economic damages were the direct and proximate result of RBS's breach of its duties.

36. RBS also had a duty to publicly disclose the data breach in a timely manner pursuant to Ga. Stat. § 10-1-910 to 912 and similar states' data breach notification statutes. Timely public disclosure was required so that, among other things, Class members could take appropriate measures to avoid fraud. Had they been informed in a more timely manner, Class members could have cancelled their cards or taken other measures to avoid fraud and identity theft. RBS breached its notification duty by failing to timely notify Class members that their personal and financial information was compromised. RBS discovered the data breach on November 10, 2008, but did not announce the breach until approximately 43 days later on December 23, 2008. RBS delayed announcing the breach until the end of the busy holiday shopping season, a period when heavy sales of gift cards occur.

37. RBS knew or should have known that its computer system for processing and storing Class members' personal and financial information was not secure.

COUNT II: BREACH OF IMPLIED CONTRACTS

38. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

39. Plaintiff and the Class entered into implied contracts with RBS such that RBS agreed to properly safeguard their personal and financial information.

40. The implied contracts were based on, *inter alia*, RBS's Privacy Policy, which stated that consumers' personal and financial information would be

safeguarded from unauthorized individuals.

41. Without such implied contracts, Plaintiff and Class members would not have provided their personal and financial information to RBS or conducted business with RBS.

42. RBS breached its implied contracts by failing to maintain adequate data security.

43. As a result of these breaches, Plaintiff and the Class have been harmed as alleged herein.

**COUNT III: VIOLATION OF THE GEORGIA
UNIFORM DECEPTIVE TRADE PRACTICES ACT,
GA. STAT. § 10-1-370 TO 375**

44. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as if fully set forth herein.

45. RBS's conduct, including but not limited to its representations regarding the adequacy of data security in light of its data security shortfalls, constituted deceptive practices under Ga. Stat. § 10-1-372(a).

46. "Proof of monetary damage, loss of profits, or intent to deceive is not required." Ga. Stat. § 10-1-373(a).

47. Plaintiff and the Class are entitled to injunctive relief under Ga. Stat. § 10-1-373(a), 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.

48. Plaintiff and the Class are entitled to recover litigation costs and attorneys' fees under Ga. Stat. § 10-1-373(b)(2) to the extent that RBS willfully failed to maintain adequate data security.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, respectfully requests the following relief:

A. that this Court certify this action as a Class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint Plaintiff and his counsel to represent the Class;

B. that this Court enter judgment in favor of Plaintiff and the Class, and against Defendant under the legal theories alleged herein;

C. that this Court award damages (including statutory damages) to Plaintiff and the Class under the legal theories alleged herein;

E. that this Court award injunctive relief including but not limited to: (i) the provision of credit monitoring services and/or identity theft insurance; and (ii) the requirement that Defendant enhance the security of its computer system to minimize the likelihood of intrusions in the future;

F. that this Court award attorneys' fees, expenses, and costs of this suit;

G. that this Court award pre-judgment and post-judgment interest at the maximum rate allowable by law; and

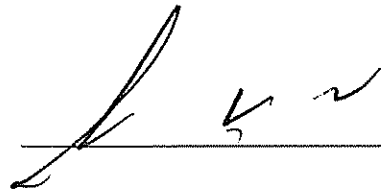
H. that this Court award such other and further relief as it may deem just and appropriate.

JURY TRIAL DEMAND

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

Dated: 1, 6-09

Respectfully Submitted,



DOFFERMYRE SHIELDS
CANFIELD & KNOWLES, LLC
Ralph I. Knowles
Georgia State Bar No. 426721
Everette . Doffermyre
Georgia State Bar No. 224750
1355 Peachtree Street
Suite 1600
Atlanta, GA 30309
Tel: (404) 881-8900
Fax: (404) 881-3007

*Liaison Counsel for Plaintiff and the
Class*

BERGER & MONTAGUE, PC
Sherrie R. Savett
Michael T. Fantini
Jon Lambiras

1622 Locust Street
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604

Counsel for Plaintiff and the Class

SHELLER, P.C.
Jamie Sheller
1528 Walnut St., 3rd Floor
Philadelphia, PA 19102
Tel: (215) 790-7300
Fax: (215) 546-0942

Counsel for Plaintiff and the Class