

10cv4822
DSD/JJK

STATE OF MINNESOTA
HENNEPIN COUNTY

DISTRICT COURT
FOURTH JUDICIAL DISTRICT

Case Type: Other Civil

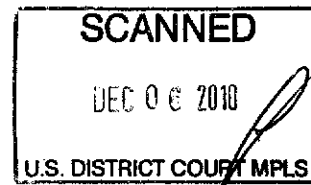
| | |
|--|----------------|
| E-SHOPS CORP., an Arizona Corporation dba PAINTBALL PUNKS, individually and on behalf of all those similarly situated, | Case No. |
| Plaintiff, | <u>SUMMONS</u> |
| v. | |
| U.S. BANK, NATIONAL ASSOCIATION, | |
| Defendant. | |

THE STATE OF MINNESOTA, To the above-named Defendant:

YOU ARE HEREBY SUMMONED and required to serve upon Plaintiff's attorneys an Answer to the Complaint which is herewith served upon you within twenty (20) days after service of this Summons upon you, exclusive of the day of service. If you fail to do so, Judgment by default will be taken against you for the relief demanded in the Complaint.

GREEN WELLING, P.C.

ROBERT S. GREEN, ESQ.
JAMES R. NOBLIN, ESQ.
595 Market Street, Suite 2750
San Francisco, CA 94105
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
rsg@classcounsel.com
jrn@classcounsel.com



ZIMMERMAN REED, PLLP

By: 

J. GORDON RUDD, JR., ESQ.

(MN No. 222082)

DAVID M. CIALKOWSKI, ESQ.

(MN No. 306526)

651 Nicollet Mall, Suite 501

Minneapolis, MN 55402

Telephone: (612) 341-0400

Facsimile: (612) 341-0844

gordon.rudd@zimmreed.com

david.cialkowski@zimmreed.com

*Attorneys for Paintball Punks,
individually, and on behalf of all class of
similarly situated individuals*

STATE OF MINNESOTA

DISTRICT COURT

HENNEPIN COUNTY

FOURTH JUDICIAL DISTRICT

Case Type: Other Civil

| | |
|---|---|
| <p>E-SHOPS CORP., an Arizona Corporation dba PAINTBALL PUNKS, individually and on behalf of all those similarly situated,</p> <p style="text-align: center;">Plaintiff,</p> <p>v.</p> <p>U.S. BANK, NATIONAL ASSOCIATION,</p> <p>Defendant.</p> | <p>Case No.</p> <p style="text-align: center;"><u>COMPLAINT</u></p> <p style="text-align: center;">DEMAND FOR JURY TRIAL</p> <p style="text-align: center;"><u>CLASS ACTION</u></p> |
|---|---|

CLASS ACTION COMPLAINT

Plaintiff E-Shops Corp. dba Paintball Punks, (“Paintball Punks” or “Plaintiff”), by and through its undersigned attorneys, brings this class action complaint against Defendant on behalf of itself and all others similarly situated based on losses suffered as a result of Defendant’s failure to remedy known data breaches in its own system. Despite its knowledge of those breaches, Defendant allowed compromised card accounts to remain active, which led to fraudulent credit card transactions with Plaintiff and others similarly situated, followed by chargebacks that Defendant processed against the accounts of Plaintiff and others similarly situated. For its class-action complaint, Plaintiff alleges as follows on personal knowledge regarding itself and its own acts and experiences, and, regarding all other matters, on information and belief, including the investigation conducted by its attorneys.

PARTIES

1. Plaintiff Paintball Punks is a corporation organized in Arizona that sells paintball equipment nationwide over the internet.

2. Defendant U.S. Bank, N.A. ("U.S. Bank") is a national banking association with its headquarters at 800 Nicollet Mall, Hennepin County, Minneapolis, Minnesota and that is located in Minnesota pursuant to 28 U.S.C. § 1348.

JURISDICTION & VENUE

3. Venue is proper under Minn. Stat. § 542 because Plaintiff's cause of action or some part thereof arose in this county.

4. This Court has personal jurisdiction over Defendant.

FACTUAL BACKGROUND

5. U.S. Bank is one of the largest credit card issuers in the United States. U.S. Bank's credit card portfolio includes over \$16 billion in loans. Its "Payment Services" line of business, which that includes credit cards, debit cards, consumer lines of credit and merchant processing services and other related items, contributed \$180 million of net income to the company for the three months of its second quarter in 2010. U.S. Bank's overall net income attributable to U.S. Bancorp for just the first half of 2010 was over \$1.4 billion.

6. Paintball Punks is a small family owned and operated internet seller located in Lake Havasu City, Arizona. Its products can be viewed at www.paintballpunks.com. Virtually all of Paintball Punk's transactions involve sales of products to customers who place orders through its website. In credit card

parlance, this type of transaction is referred to as a "card not present" or "CNP" transaction.

7. Merchants who run CNP transactions utilize several security devices to avoid fraudulent transactions. Before shipping goods to any customer, Paintball Punks runs through the available security checks to avoid fraudulent transactions. One of the security operations it performs is known as an address verification or "AVS" check. This process compares the customer's address and ZIP code provided in the order form with the address and ZIP code on file for the cardholder at U.S. Bank, or whatever bank issued the credit card. Paintball Punks also performs a card verification code or "CVC2" check, which requires the customer to provide the three- digit code written at the end of the card number on top of the card's signature strip. Additionally, Paintball Punks will only ship the requested products to the address that is on file at U.S. Bank (or the other issuing bank) as the cardholder's billing address and it requires a hard signature receipt for product delivery to occur.

8. The credit card processing system often involves five players: (1) the merchant who offers goods or services for sale, (2) the merchant's processor that keeps track of data on the merchant's transactions and distributes the data into the financial system, (3) the merchant's bank (often referred to as the "acquiring bank"), (4) the credit cardholder's bank (often referred to as the "issuing bank" because it issued the credit card), and (5) the cardholder.

9. In a typical internet transaction, the cardholder orders goods through an online form, the merchant processes the transaction and ships the goods, and the processor provides the information to the issuing bank, which sends funds to the merchant's bank, which in turn deposits the funds into the merchant's account.

The issuing bank then adds that transaction to the cardholder's bill, which is then sent to the cardholder in the ordinary course.

10. When cardholders receive a bill describing transactions they did not authorize, they can object to the transaction under the Fair Credit Billing Act, 15 U.S.C. §1601, *et seq.* Under standard credit card network rules discussed below, the issuing bank then initiates a "chargeback" to the merchant bank, which causes the merchant bank to return to the issuing bank any funds that it had received for the transaction. Each bank settles to the issuing bank. And they each then settle up with their own customers according to their respective agreements. For the transactions at issue in this case, as is typical, Paintball Punk's bank withdrew the funds from its bank account and returned those funds to U.S. Bank.

11. Visa's operating guidelines provide guidance to the parties on how to process transactions and chargebacks. Visa's chargeback rules purport to allocate the risk of fraudulent transactions between the issuing bank and the acquiring bank, and thus, ultimately to the cardholder and the merchant, based upon a judgment of whose conduct created the dispute that resulted in the chargeback. In the typical situation, since it is the merchant that is dealing directly with the customer, the merchant would have the ability to prevent fraudulent transactions and it would be the merchant's bank and ultimately the merchant that suffers the risk of loss. However, in this case, it is U.S. Bank's wrongfully self-interested conduct that generated the disputes that resulted in chargebacks.

12. Before the events at issue in this case, Paintball Punks successfully avoided chargebacks by using the standard security devices, summarized above, that were available for CNP transactions. Beginning in approximately August 2009, however, Plaintiff began experiencing chargebacks on cards issued by U.S.

Bank. Subsequent investigation of chargebacks on the U.S. Bank issued cards included conversations with two U.S. Bank employees who admitted that the bank's system had been compromised. Plaintiff was informed by these employees that U.S. Bank was well aware of the problem and that it had been going on for a while. Those employees also advised Plaintiff that U.S. Bank knows when fraudulent orders come through the system, because the cardholder typically has processed a change of address shortly before placing a large volume of orders on several different websites.

13. During the period from August through December of 2009, Plaintiff received nine fraudulent orders from cardholders paying with U.S. Bank credit cards for a total amount of \$11,259.91 of merchandise, an average of \$1,251.10 per order. In each case, Plaintiff ran the AVS check by which U.S. Bank confirmed that the shipping address was the same as the billing address in its system. Plaintiff also performed the CVC2 check, which verified the three-digit code on the individual credit cards. This means that the only way that these transactions could be fraudulent is if the purchaser either had seen the back of the credit card or had obtained the code from the records of the credit-card issuer. Plaintiff then shipped the goods and obtained a receipt signature from a person at the address that U.S. Bank had confirmed as the cardholder's billing address. In connection with each transaction, the data was passed through Plaintiff's processor to U.S. Bank, which then sent the applicable funds to Plaintiff's bank (HSBC Bank), where it was deposited into Plaintiff's account.

14. With regard to each of these nine transactions, the cardholders submitted an objection to U.S. Bank contesting the charges on their credit card account. U.S. Bank then initiated "chargebacks," a "chargeback" which caused

Plaintiff's bank to send the amount of each transaction, the \$11,259.91 in total, back to U.S. Bank and, of course, to deduct those amounts from Plaintiff's account.

15. The chargebacks processed by U.S. Bank with regard to Plaintiff included as many as 15 transactions in a single account over a period of 13 days. One of the U.S. Bank cardholders, for example, contested 15 charges for a total of \$14,279.52 from the following merchants located in the following states:

| | |
|----------------------------|----|
| Paintball Punks | AZ |
| Action Village | IL |
| A.N.S. Xtreme Performa | CA |
| Zephyr Sports | CA |
| Staples Direct | CA |
| Compulsive Paintball | PA |
| Action Village | IL |
| Action Village | IL |
| Staples Direct | CA |
| Paintball Punks | AZ |
| Buydig | NJ |
| Nordstrom Direct | IA |
| A.N.S. Xtreme Performa | CA |
| Nordstrom Direct | IA |
| <u>www.RalphLauren.com</u> | PA |

DATA BREACHES IN THE CREDIT CARD INDUSTRY

16. Because of the value of stolen credit card numbers, data breaches in the credit card industry have been increasingly frequent over the last several years. Sometimes the breach occurs at the merchant (as in the cases of DSW Shoes and TJ Maxx). In that case, a thief would gain access to information about customers that patronize a particular merchant. In other cases (as in the Heartland case), the breach occurs at the processor; in that case, a thief would gain access to information about customers patronizing merchants that use that particular processor. Still another possibility is that the breach would occur at the issuing

bank; in that case, a thief would gain access to information about customers with cards issued by that particular bank.

17. Each of the unusual chargebacks in this case involved a card issued by U.S. Bank. The great majority of card transactions do not involve U.S. Bank cards; only about 8% of spending on credit cards in this country last year was made with U.S. Bank cards. Thus, the most likely explanation, consistent with the explanation of the U.S. Bank employees mentioned above, is that the fraudulent activity resulted from a data breach at U.S. Bank.

18. U.S. Bank could have corrected the data breach at several points before the losses suffered by Plaintiff and the members of the class. First, when it learned of the breach it could have notified all of the affected cardholders at once and cancelled their cards at that time. In that case, none of the information obtained in the breach could have been used to defraud Plaintiff.

19. U.S. Bank, however, had (and continues to have) strong incentives to cover up the data breach. Credit and debit card fraud is a paramount concern of Americans in the midst of the global financial crisis. Concern about fraud supersedes that of terrorism, computer and health viruses and personal safety. (Source: Unisys Security Index: United States, March 2009).

20. Currently, U.S. Bank is an industry leader in customer satisfaction. According to J.D. Power and Associates 2010 Credit Card Satisfaction Study Rankings, U.S. Bank ranked third of all major card issuers, behind only American Express and Discover, and ahead of Wells Fargo, Chase, Citibank, Bank of America and all other major card issuers.

21. If U.S. Bank were to notify large numbers of its cardholders of a data breach in its facilities, then it would stoke the fears and concerns of credit

card fraud among its cardholders, and they would associate that fear with U.S. Bank as an issuer. That association would seriously damage U.S. Bank's position as one of the top three credit card issuers with regard to customer satisfaction. That in turn would seriously jeopardize the hundreds of millions of dollars of net profit that U.S. Bank currently earns from its card operations. One likelihood is that many of the affected cardholders would be likely to switch their usage to a card issued by another bank. Second, more generally, information about the fraud could seriously damage U.S. Bank's currently high reputation in the industry. That damage could affect U.S. Bank for years to come in its efforts to compete with other issuers for the business of its cardholders and other potential customers.

22. Third, notifying the public of U.S. Bank's poor data security and its failure to take proper corrective action upon learning of the data breach would expose U.S. Bank to potential liability to the merchants to whom the fraudulent charges were passed by the chargeback procedure. By failing to notify the public of the facts regarding its lack of data security, U.S. Bank attempted to shift the loss resulting from that defect from itself to the merchants.

23. U.S. Bank also could have taken action – notifying its cardholders and cancelling accounts – when it first learned that the data breach was leading to fraudulent transactions. Once it understood that the stolen data was being used to conduct fraudulent transactions, the likely harms to third parties like Plaintiff was much higher. Yet U.S. Bank still took no action even when fraudulent transactions began to appear.

24. Apparently, U.S. Bank determined that it would respond to the data breach in a wholly reactive manner, terminating cards on a case-by-case basis only after customers complained about fraudulent transactions. Because many of the

frauds (including the ones about which Paintball Punks complains) involve accounts on which the thief successfully changed the billing address, those frauds likely would continue for several months – because statements would be mailed to the thief rather than the original cardholder. The original cardholder likely would discover the problem only if it examined the statement online or if U.S. Bank contacted the cardholder to inquire about nonpayment (a likely circumstance if bills are mailed to the thieves instead of the cardholders). The end result, summarized above, was a large and wholly avoidable set of fraudulent purchases from Plaintiff and others similarly situated.

CLASS ALLEGATIONS

25. Plaintiff brings this action pursuant to Minnesota Rule of Civil Procedure 23 on behalf of the following (the “Class”):

All merchants in the United States that received chargeback claims from U.S. Bank with regard to cards that were the subject of a data breach at U.S. Bank or its affiliates.

26. The members of the Class are so numerous and geographically dispersed that joinder of all members of the Class would be impracticable. Members of the Class are located throughout the United States. The exact number of the members of the Class is unknown to Plaintiff at this time, but Plaintiff reasonably believes the Class to number at least in the hundreds or thousands.

27. Plaintiff's claims are typical of the members of the Class. Plaintiff and all members of the Class were commonly impacted and damaged by Defendant's wrongful conduct. Plaintiff and the members of the Class were

subjected to chargebacks that resulted from or related to the breach in Defendant's data security.

28. The class is readily ascertainable from Defendant's own records. The fraudulent purchasers apparently changed the billing address for the credit cards in question shortly before charging over one thousand dollars in purchases with rush shipping fees. A review of Defendant's records would determine the set of transactions that occurred in accounts that had been the subject of a data breach, which could be further narrowed to transactions that occurred after a) a particular credit card's billing address was changed b) shortly before purchases were made in amounts exceeding one thousand dollars c) with subsequent chargebacks resulting d) after the Defendant determined that the billing address was inaccurate, and e) efforts were made to contact the actual cardholder.

29. Plaintiff will fairly and adequately protect the interests of the Class. The interests of Plaintiff are coincident with, and not antagonistic to, those of the Class. In addition, Plaintiff's counsel is experienced and competent in prosecuting complex class action litigation. Plaintiff and its counsel are committed to prosecuting vigorously this action on behalf of the other members of the Class, and have the financial resources to do so. Neither Plaintiff nor its counsel has any interest adverse to the other members of the Class.

30. Absent a class action, members of the Class would find the cost of litigating their claims to be prohibitive, and will have no effective remedy. Class treatment of common questions of law and fact also is superior to multiple individual actions or piecemeal litigation, in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

31. The Class has a high degree of cohesion, and prosecution of the action through class representatives would be unobjectionable. Plaintiff is not aware of any other difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

32. The factual and legal bases of Defendant's liability to Plaintiff and to the Class are the same, resulting in injury to the Plaintiff and to the Class. Plaintiff and the other members of the Class all have suffered harm and damages as a result of Defendant's unlawful and wrongful conduct.

33. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual members of the Class. Questions of law and fact common to the Class include, but are not limited to the following:

- a. What Defendant knew about the breach of its data security;
- b. What Defendant knew about fraudulent orders placed by those taking advantage of the data breach;
- c. Whether those placing the fraudulent orders committed a tort against members of the class;
- d. Whether Defendant substantially assisted in the commission of the tort by processing the transactions in question rather than notifying cardholders of the data breach and/or blocking the data breach;
- e. Whether Defendant's conduct constituted aiding and abetting fraudulent transactions;
- f. Whether Defendant's conduct constituted tortious interference;
- g. Whether Defendant intentionally interfered with the Class's Class Members' contracts with its/their merchant banks;
- h. Whether Defendant's conduct was justified; and
- i. Whether the circumstances amount to unjust enrichment of Defendant that warrants restitution caused harm to the Class.

34. In the alternative, the Class may be certified pursuant to Minn. R. Civ. P. 23.02(a) or 23.02(b) because:

- a. The prosecution of separate actions by the individual members of the Classes would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant;
- b. The prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which 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; and,
- c. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the members of the Class as a whole.

COUNT I
AIDING AND ABETTING FRAUDULENT TRANSACTIONS

35. Plaintiff restates and realleges all paragraphs above as though set forth in full herein.

36. Individuals obtained credit card data from U.S. Bank and fraudulently used that information to purchase goods in transactions with Plaintiff and the other members of the Class.

37. Defendant was aware that such fraudulent transactions were being conducted with information stolen from its system that involved address changes on the credit card accounts that made it highly likely that merchants would approve those transactions followed by a series of internet purchases.

38. Defendant substantially assisted in the fraudulent transactions by not correcting the data breach at the time it occurred and by providing false

information into the security check system that merchants use to avoid fraudulent transactions.

39. Plaintiff seeks damages, in an amount yet to be determined, together with costs and disbursements, including costs of the investigation and reasonable attorneys' fees, and any other equitable relief (including disgorgement, restitution, imposition of constructive trust, and an accounting) that may be appropriate against Defendant for its conduct.

COUNT II
INTENTIONAL INTERFERENCE WITH CONTRACTUAL
RELATIONS WITH MERCHANT BANK

40. Plaintiff restates and realleges all paragraphs above as though set forth in full herein.

41. Plaintiff had a contract with HSBC bank pursuant to which HSBC bank acted as Plaintiff's merchant bank for credit card transactions between Plaintiff and its customers in return for certain fees and charges. Under that contract, HSBC deposited funds into Plaintiff's account upon receipt of certain processing information and authorizations. On the rare occasions when an issuing bank initiated a chargeback, HSBC would withdraw the funds from Plaintiff's account and return them to the issuing bank, leaving Plaintiff, the issuing bank, the card holder and the purchaser to resolve the issue of what money should be paid to plaintiff as a result of a given transaction.

42. Defendant was aware of Plaintiff's contract with HSBC bank, having delivered monies to HSBC bank for other credit card transactions between Plaintiff and purchasers before the transactions in question. Further, Defendant is also aware because of Defendant's transactions as an issuing bank that many

merchants have contracts with HSBC bank similar to Plaintiff's. Moreover, Defendant is also aware, because of the information transmitted between merchant banks and issuing banks, that HSBC is Plaintiff's merchant bank for credit card transactions.

43. Defendant's conduct as alleged in this Complaint constitutes intentional interference with Plaintiff's contract with HSBC bank. Defendant knew that the security of its data had been breached and could have responded by either blocking the data breach or by notifying cardholders of the data breach and directing them either a) to obtain cards from other sources or b) to obtain new cards from Defendant in a secure data system. Instead, Defendant allowed fraudulent purchasers to take advantage of the breach of data security to obtain Plaintiff's product by charging the purchase to cardholders whom the fraudulent purchasers knew would not pay for items that the cardholders themselves had not ordered. Further, Defendant affirmatively provided Plaintiff with AVS information, confirming that the shipping address on the order placed by fraudulent purchasers was the same as the billing address for the credit card and verifying the 3 digit CVC2 code the fraudulent purchaser had entered, even though Defendant knew that such information was false when entered by a fraudulent purchaser who had obtained the relevant data as a result of the breach of Defendant's data security.

44. Defendant's conduct was without justification. Rather than bear the cost of fixing the breach in its data security or the loss resulting from notifying cardholders of the breach, Defendant decided to impose on Plaintiff the loss of fulfilling orders placed by fraudulent purchasers.

45. As a result of Defendant's conduct, Plaintiff was harmed in that Plaintiff shipped product ordered by fraudulent purchasers for a specified amount and then suffered monetary loss when that amount was transferred out of Plaintiff's account and transmitted back to Defendant as a result of the chargebacks initiated by Defendant after cardholders were informed of the fraudulent purchase on their credit cards. Consequently, Plaintiff's performance of its contract with HSBC bank was made needlessly more expensive than would otherwise be the case when Plaintiff shipped products for which, after the deduction of funds from its account pursuant to the chargeback procedure, Plaintiff was not paid.

46. Plaintiff seeks damages, in an amount yet to be determined, along with costs and disbursements, including costs of investigation and reasonable attorneys' fees, and any other equitable relief (including disgorgement, restitution, imposition of a constructive trust, and an accounting) against Defendant for its conduct.

COUNT III
VIOLATION OF MINNESOTA'S CONSUMER
PROTECTION STATUTES
Minn. Stat. §§ 325F.69, subd. 1, and 325D.44, subd. 1(13)

47. Plaintiff restates and realleges all paragraphs above as though set forth in full herein.

48. U.S. Bank failed adequately to secure its customers' account data. When U.S. Bank's security apparatus was breached, and those breaching the system procured U.S. Bank customers' account data, U.S. Bank was aware of the problem. U.S. Bank then engaged in a deceptive practice, in violation of

Minnesota Statutes §§ 325F.69, subd. 1, and 3225D.44, subd. 1(13), by failing to notify the affected cardholders and cancelling their cards.

49. This material omission constituted deceptive practices against cardholders, who would naturally believe their data were safe unless told otherwise by the only party that could have such knowledge—U.S. Bank. Instead, U.S. Bank's decision not to cancel cardholders' accounts, and not to inform cardholders' of the security breach so that they could initiate such cancellations themselves, caused the cards not to be cancelled and allowed the security breach to advance to the reasonably foreseeable stage of the breacher using customers' data to engage in fraudulent transactions with customers' cards. Thus, the resulting fraudulent transactions were made in direct connection with the deceptive practices of U.S. Bank.

50. These material omissions caused Plaintiff and class members to incur chargebacks through no fault of their own as described, *supra*.

51. U.S. Bank's decision to keep secret these material facts was aimed at its cardholding customer base at large, and therefore the successful prosecution of this case will advance state interests, even if the group of persons benefitting from monetary relief obtained through the lawsuit is small.

52. Under Minnesota law, pursuant to Minnesota Statute § 8.31, subd. 3a, neither Plaintiff nor class members need to plead or establish direct evidence of reliance by individual cardholders in order to establish the causal nexus between U.S. Bank's material omissions and the chargebacks imposed on Plaintiff and class members, and Plaintiff does not so plead here. Rather, Plaintiff asserts that there is a causal nexus between the deceptive practice and the injury

to Plaintiff that can be proven by other circumstantial evidence of causation that is not individualized in nature.

53. By reason of such violations and pursuant to Minn. Stat. § 8.31, subd. 3a and § 325D.44 and § 325D.45, Plaintiff demands compensatory damages, attorneys' fees and costs, injunctive and equitable relief, and other remedies as determined by the Court pursuant to Minn. Stat. § 8.31, subd. 3a and §325D.45. Minn. Stat. § 325D.44 is, by title and on its face, a law of Minnesota respecting "unfair" and "other unlawful practices in business, commerce, or trade" and is a law "against false or fraudulent advertising." Minn. Stat. §8.31, subd. 1.

COUNT IV
RESTITUTION/UNJUST ENRICHMENT

54. Plaintiff restates and realleges all paragraphs above as though set forth in full herein.

55. Plaintiff and the Class have conferred a direct benefit on Defendant. Defendant received and retained money, through a profit share or otherwise, belonging to Plaintiff and the Class resulting from Defendant's conduct.

56. Defendant has knowledge of this benefit and the fact that some of the monies it received and continues to receive are resulting from its chargebacks.

57. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class by which Defendant has been unjustly enriched as a result of Defendant's actions more fully described above.

58. As a result of Defendant's retention of money belonging to Plaintiff and the Class, Plaintiff and the Class suffered, and will continue to suffer,

damages, in an amount yet to be determined, but reasonably believed to be greater than \$50,000.00 (fifty thousand dollars).

WHEREFORE, Plaintiff on behalf of itself and the Class pray for the following relief:

- a) Certification of this case as a class action on behalf of the Class as defined above, appointment of Paintball Punks as Class Representative, and appointment of undersigned counsel as lead class counsel;
- b) A Declaration that the actions of Defendant, as set forth above, violate Minnesota law and constitute unjust enrichment, as set forth above;
- c) Entry of judgment against Defendant for all actual, monetary, economic, consequential, and compensatory damages in an amount yet to be determined, but in an amount greater than \$50,000, caused as a result of its unlawful conduct;
- d) An Order for injunctive, declaratory, and equitable relief as necessary against Defendant to protect the interests of Plaintiff and the Class, including an entry of an injunction prohibiting continuation or repetition of the acts alleged above, as well as disgorgement, restitution, imposition of a constructive trust, and an accounting;
- e) An award to Plaintiff and the Class of their reasonable costs and attorneys' fees; and,
- f) An award of any further relief that equity and justice may require.

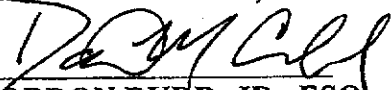
JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

GREEN WELLING, P.C.

ROBERT S. GREEN, ESQ.
JAMES R. NOBLIN, ESQ.
595 Market Street, Suite 2750
San Francisco, CA 94105
Telephone: (415) 477-6700
Facsimile: (415) 477-6710
rsg@classcounsel.com
jrn@classcounsel.com

ZIMMERMAN REED, PLLP

By: 
J. GORDON RUDD, JR., ESQ.
(MN No. 222082)
DAVID M. CIALKOWSKI, ESQ.
(MN No. 306526)
651 Nicollet Mall, Suite 501
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
gordon.rudd@zimmreed.com
david.cialkowski@zimmreed.com

*Attorneys for Paintball Punks,
individually, and on behalf of all class of
similarly situated individuals*

ACKNOWLEDGMENT

The undersigned hereby acknowledges that costs, disbursements, and reasonable attorney and witness fees may be awarded to the party against whom the allegations in this pleading are asserted pursuant to Minn. Stat. § 549.211.

Dated: 11/5/2010

PERSONALLY SERVED
11/5/10 @ 10:00AM
US BANK (KJC)



ZIMMERMAN REED
ATTORNEYS AT LAW

November 4, 2010

Via Hand Delivery

U.S. Bank, National Association
c/o CT Corporation System, Inc.
100 S. 5th St., Suite 1075
Minneapolis, MN 55402

TINA M. OLSON
Tina.Olson@zimmreed.com

REPLY TO MINNEAPOLIS


RE: *E-Shops Corp., et al. v. U.S. Bank, National Association*

Dear Sir or Madam:

Enclosed herewith and served upon you please find the Summons and Complaint filed in the above-entitled matter.

Very truly yours,

ZIMMERMAN REED, P.L.L.P.


Tina M. Olson
Paralegal

enc.