

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA**

BRIAN NOWE, on behalf of himself and
all others similarly situated,

Plaintiff,

v.

ESSEX TECHNOLOGY GROUP, LLC
(d/b/a Bargain Hunt); and DOES 1
through 20, inclusive,

Defendants.

CASE NO._____

**COMPLAINT -- CLASS ACTION
JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff, by his counsel of record, brings this action individually and on behalf of all others similarly situated, pursuant to Federal Rule of Civil Procedure 23 and Northern District of Georgia Local Rule 23, and alleges the following upon personal knowledge, or where there is not personal knowledge, upon information and belief:

PRELIMINARY STATEMENT

1. Plaintiff on behalf of himself and all others similarly situated brings this action against Essex Technology Group, LLC and Does 1 through 20 (all named and Doe defendants collectively referred to as "Defendants") based on Defendants' violations of the Fair and Accurate Credit Transactions Act ("FACTA"), 15 U.S.C. §§ 1681 *et seq.*

2. FACTA provides in relevant part that "**no person** that accepts credit cards or debit cards for the transaction of business **shall print more than the last 5 digits of the card number . . . upon any receipt provided to the cardholder** at the point of the sale or transaction." 15 U.S.C. § 1681c(g)(1) (emphasis added).¹

3. The FACTA law gave merchants who accept credit and or debit cards up to three years to comply with its requirements, requiring full compliance with its provisions no later than December 4, 2006. Although Defendants had up to

¹ As the United States Government explained in its brief in support of FACTA's truncation provisions filed in *Papazian v. Burberry Ltd.*, 2:07-cv-01479-GPS-RZ (C.D. Cal.), Congress' decision to enact FACTA followed many other state legislatures, including those of Georgia, who had already enacted state laws prohibiting merchants from printing the expiration date or more than the last 5 digits of the card on customer receipts. Exhibit 3 at pp. 13-14 and n. 2 and 3, citing Ga. Code Ann. § 10-15-3 which provides that "A merchant who accepts a payment card for the transaction of business shall not print more than five digits of the payment card's account number or print the payment card's expiration date on a receipt provided to the cardholder."

three years to comply, Defendants willfully violated this law and failed to protect Plaintiffs and others similarly situated against identity theft and credit and debit card fraud by printing more than the last 5 digits of the card number on receipts provided to credit card and/or debit card cardholders transacting business with Defendants. More specifically, Defendants printed the first 6 digits and the last 4 digits of the credit and/or debit card number on credit and/or debit card receipts. This conduct is in direct violation of FACTA.

4. Nor is Defendants' willful violation of FACTA a trifling matter. In the statement provided during his signing of FACTA in 2003, the President underscored the importance of the legislation in combating rampant identity theft:

This bill also confronts the problem of identity theft. A growing number of Americans are victimized by criminals who assume their identities and cause havoc in their financial affairs. With this legislation, the Federal Government is protecting our citizens by taking the offensive against identity theft.

5. Courts have likewise emphasized the purpose of FACTA. For example, the Ninth Circuit recently emphasized that "[i]n fashioning FACTA, Congress aimed to 'restrict the amount of information available to identity thieves.'" *Bateman v. American Multi-Cinema, Inc.*, 623 F.3d 708, 718 (9th Cir. 2010) (quoting 149 Cong. Rec. 26,891 (2003) (statement of Sen. Shelby)).

6. Similarly, the Seventh Circuit recently explained that "[i]dentity theft is a serious problem, and FACTA is a serious congressional effort to combat it." *Redman v. Radioshack Corp.*, 768 F.3d 622, 639 (7th Cir. 2014).

7. Moreover, despite many defendants' attempts to label FACTA violations as "technical," the Ninth Circuit has squarely rejected such arguments and held that such a violation "is not merely 'technical.'" *Bateman*, 623 F.3d at 714 and n.4. Plaintiff's situation is exactly the scenario Congress sought to avoid by passing FACTA.

8. Further, by printing the first 6 and last 4 digits of the card number on the receipts provided to Plaintiff and other credit card and/or debit card cardholders transacting business with Defendants, Defendants have harmed Plaintiff and the Class by exposing them to at least an increased and material risk of identity theft and credit and or debit card fraud.

9. For example, the first 6 and last 4 digits of the card number can be used to bolster the credibility of a criminal who is making pretext calls to a card holder or engaging in e-mail phishing scams in order to learn other personal confidential financial information.

10. As the United States Government explained in its brief in support of FACTA's truncation provisions filed in *Papazian v. Burberry Ltd.*, 2:07-cv-01479-

GPS-RZ (C.D. Cal.): "Congress' decision to protect both card numbers and expiration dates from inadvertent disclosure through discarded sales receipts, as many states had already done, directly serves the interest Congress sought to protect" particularly since "***Thieves might piece together (or 'pick off,' in the words*** of Congress) different bits of information from different sources." See Exhibit 3 at pp. 13-16; see also intervention by United States in *Harris v. Mexican Specialty Foods, Inc.*, 564 F.3d 1301, 1307 (11th Cir. 2009).

11. Indeed, the fact that thieves can piece together card information was recently demonstrated by computer scientists who released a study showing how "even starting with no details at all other than the first six digits [of a card number] a hacker can obtain the three essential pieces of information to make an online purchase within as little as six seconds." See Exhibit 1 at p. 2: Six Seconds To Hack A Credit Card (<http://www.ncl.ac.uk/press/news/2016/12/cyberattack/>). These computer scientists' study showed that starting with nothing more than the first 6 digits of a card number, and "By automatically and systematically generating different variations of the cards security data and firing it at multiple websites, within seconds hackers are able to get a 'hit' and verify all the necessary security data." Exhibit 1 at p. 2; and Exhibit 2: Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?, Mohammed Aamir Ali, et al.,

(http://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf). "Investigators believe this guessing attack method is likely to have been used in the recent Tesco cyberattack which defrauded customers of £2.5m." Exhibit 1 at p. 2.

12. Nor is this harm made harmless when the risk fails to materialize because no potential identity thief actually sees the receipt. Even in this situation, the consumer (such as Plaintiff and Class members) must take additional steps to ensure the safety of his or her identity; he or she may not simply crumple the receipt and throw it into a nearby trash can, but must review it to assess what was printed, hold on to it, and perhaps shred it or cut it up later. The additional inconvenience that a consumer must undertake in order to secure their own rights, when a statute places that burden on Defendants, is surely a concrete harm. *Deschaaf v. American Valet & Limousine, Inc.*, 234 F.Supp.3d 964, 970 (D. Ariz. Feb. 15, 2017). "As the Seventh Circuit observed, this is why statutory damages exist. Some harms—a modest concern about privacy, a slight chance that information would leak out and lead to identity theft—are not easy to quantify, at least in any appreciable dollar amount. See *Murray v. GMAC Mortg. Corp.*, 434 F.3d 948, 953 (7th Cir. 2006). But even if they give rise to no actual *damages*, they are still actual *harms*." *Deschaaf*, 234 F.Supp.3d at 970 and n. 7. "Allowing

consumers to recover statutory damages furthers [the congressional purpose of keeping information out of the hands of identity thieves] by deterring *businesses* from willfully making consumer financial data available, even where no actual harm results." *Deschaaf*, 234 F.Supp.3d at 970 and n. 8 (alterations in original), quoting *Bateman v. American Multi-Cinema, Inc.*, 623 F.3d 708, 718 (9th Cir. 2010).

13. In sum, Defendants have violated FACTA, and have thereby placed the security of Plaintiff and similarly situated Class members at material risk. As a result of Defendants' unlawful practice of violating FACTA's provisions intended to safeguard against identity theft and credit and debit card fraud, Plaintiff seeks, on behalf of himself and the Class, statutory damages, punitive damages, costs and attorney fees, all of which are expressly made available by statute, 15 U.S.C. §§ 1681 *et seq.*

PARTIES

14. Plaintiff, Brian Nowe, is and at all times relevant hereto was a resident of the State of Georgia.

15. Defendant Essex Technology Group, LLC is a Tennessee limited liability company. Essex Technology Group, LLC owns, manages, maintains, and/or operates many physical brick-and-mortar retail store locations throughout

the State of Georgia, through which it offers various goods and services for sale to the public, and it does extensive business throughout the State of Georgia. Essex Technology Group, LLC does business using its own name as well as under other fictitious business names such as, but not limited to, "Bargain Hunt."

16. At all times mentioned in this Complaint, Defendants and each of them were the agents, employees, joint venturer, and or partners of each other and were acting within the course and scope of such agency, employment, joint venturer and or partnership relationship and or each of the Defendants ratified and or authorized the conduct of each of the other Defendants.

17. Plaintiff does not know the true names and capacities of defendants sued herein as Does 1 through 20, inclusive, and therefore sues these defendants by such fictitious names. Plaintiff is informed and/or believes that each of the Doe defendants was in some manner legally responsible for the wrongful and unlawful conduct and harm alleged herein. Plaintiff will amend this Complaint to set forth the true names and capacities of these defendants when they have been ascertained, along with appropriate charging allegations.

JURISDICTION AND VENUE

18. This Court has federal question jurisdiction pursuant to 28 U.S.C. § 1331 and 15 U.S.C. § 1681p.

19. Plaintiff's claims asserted herein arose in this judicial district and Defendants do business in and reside in this judicial district.

20. Venue in this judicial district is proper under 28 U.S.C. § 1391(b) and (c) in that Defendants have done and continue to do business, and intentionally avail themselves of the markets within this district, they own, manage, maintain and/or operate one or more physical locations within this district, and this is a class action case in which a substantial part of the acts and omissions giving rise to the claims occurred within this judicial district.

CLASS ACTION ALLEGATIONS

21. Plaintiff brings this Class action on behalf of himself and all other persons similarly situated pursuant to Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure.

22. The Class which Plaintiff seeks to represent is defined as:

All consumers to whom Defendants, after May 17, 2015, provided an electronically printed receipt at the point of a sale or transaction at any of Defendants' physical store locations in the United States, on which receipt Defendants printed more than the last 5 digits of the consumer's credit card or debit card (the "Class").²

² Plaintiff reserves the right to amend or otherwise modify the Class definition and/or add sub-classes.

23. Excluded from the Class are Defendants and each of their directors, officers, and employees. Also excluded from the Class are any justice, judge, or magistrate judge assigned to this action or who presides over any proceeding concerning this action, and any such justice's, judge's, or magistrate judge's spouse, or a person within the third degree of relationship to any of them, or the spouse of such a person.

24. Numerosity (Fed. R. Civ. P. 23(a)(1)): The Class is so numerous that joinder of all individual members in one action would be impracticable. The disposition of their claims through this Class action will benefit both the parties and this Court.

25. Plaintiff is informed and believes and thereon alleges that there are, at a minimum, thousands (*i.e.*, two thousand or more) of members that comprise the Class.

26. The exact size of the Class and identities of individual members thereof are ascertainable through Defendants' records, including but not limited to Defendants' sales and transaction records.

27. Members of the Class may be notified of the pendency of this action by techniques and forms commonly used in Class actions, such as by published notice, e-mail notice, website notice, first-Class mail, or combinations thereof, or

by other methods suitable to this Class and deemed necessary and or appropriate by the Court.

28. Typicality (Fed. R. Civ. P. 23(a)(3)): Plaintiff's claims are typical of the claims of the entire Class. The claims of Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful conduct.

29. Plaintiff and members of the Class were each customers of Defendants, each having made a purchase or transacted other business with Defendants' after May 17, 2015, using a credit card or debit card. At the point of such sale or transaction with Plaintiff and members of the Class, Defendants provided to Plaintiff and each member of the Class a receipt in violation of 15 U.S.C. §1681c(g)(1) (*i.e.*, a receipt on which is printed more than the last 5 digits of the credit or debit card).

30. Common Questions of Fact and Law (Fed. R. Civ. P. 23(a)(2) and (b)(3)): There are a well-defined community of interest and common questions of fact and law affecting the members of the Class.

31. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

(a) Whether Defendants' conduct of providing Plaintiff and the Class with sales or transaction receipts whereon Defendants printed more than the last 5 digits of the card violated the FACTA, 15 U.S.C. §§ 1681 *et seq.*;

(b) Whether Defendants' conduct was willful pursuant to 15 U.S.C. § 1681(n); and

(c) Whether Plaintiff and the Class are entitled to statutory damages, punitive damages, costs and or attorney fees for Defendants' acts and conduct.

32. Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)): Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class which Plaintiff seeks to represent. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the Class and has no interests antagonistic to the Class. Plaintiff has retained counsel who is competent and experienced in the prosecution of Class action litigation.

33. Superiority (Fed. R. Civ. P. 23(b)(1) and 23(b)(3)): A Class action is superior to other available means for the fair and efficient adjudication of the claims of the Class. While the aggregate damages which may be and if awarded to the Class are likely to be substantial, the actual damages suffered by individual members of the Class are relatively small. As a result, the expense and burden of

individual litigation makes it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. The likelihood of individual Class members prosecuting separate claims is remote. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would increase the delay and expense to all parties and the court system resulting from multiple trials of the same factual issues. In contrast, the conduct of this matter as a Class action presents fewer management difficulties, conserves the resources of the parties and the court system, and would protect the rights of each member of the Class. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a Class action.

CAUSES OF ACTION

COUNT ONE

For Violation of 15 U.S.C. §§ 1681 *et seq.*

(On Behalf of Plaintiff and the Class as against Defendants)

34. Plaintiff hereby incorporates by reference the allegations contained in this Complaint.

35. Plaintiff asserts this claim on behalf of himself and the Class against Defendants.

36. Title 15 U.S.C. § 1681c(g)(1) provides that "no person that accepts credit cards or debit cards for the transaction of business shall print more than the last 5 digits of the card number or the expiration date upon any receipt provided to the cardholder at the point of the sale or transaction."

37. By its express terms, 15 U.S.C. § 1681c(g)(1) applies to "any cash register or other machine or device that electronically prints receipts for credit card or debit card transactions" after December 3, 2006. 15 U.S.C. § 1681c(g)(3).

38. Defendants transact business in the United States and accept credit cards and debit cards in the course of transacting business with persons such as Plaintiff and members of the Class. In transacting such business, Defendants use cash registers and or other machines or devices that electronically print receipts for credit card and debit card transactions.

39. After May 17, 2015, and within two years from the date of filing this action, Defendants, at the point of a sale or transaction with Plaintiff Brian Nowe, provided Plaintiff Brian Nowe with one or more electronically printed receipts on each of which Defendants printed more than the last 5 digits of his credit card number. More specifically, Defendants printed the first 6 digits and the last 4 digits of Plaintiff Brian Nowe's credit card number on his customer receipt(s).

40. After May 17, 2015, Defendants, at the point of a sale or transaction with members of the Class, provided each member of the Class with one or more electronically printed receipts on each of which Defendants printed, for each respective Class member, more than the last 5 digits of their credit card or debit card number.

41. As set forth above, FACTA was enacted in 2003 and gave merchants who accept credit and or debit cards up to December 4, 2006 to comply with its requirements.

42. Defendants knew of and were well informed about the law, including specifically FACTA's requirements concerning the truncation of credit and debit card numbers and prohibition on the printing of expiration dates.

43. For example, but without limitation, several years ago, VISA, MasterCard, the PCI Security Standards Council (a consortium founded by VISA, MasterCard, Discover, American Express and JCB), companies that sell cash register and other devices for the processing of credit or debit card payments, companies that sell software to operate payment card devices, companies that maintain and repair hardware or software used to process payment card transactions, and other entities informed Defendants about FACTA, including its specific requirements concerning the truncation of credit and debit card numbers

and prohibition on the printing of expiration dates, and Defendants' need to comply with same.

44. Other entities, including but not limited to Defendants' payment card processor (also known as the acquirer, merchant bank, or acquiring bank) which processes credit and debit card payments for transactions occurring at Defendants' stores, likewise informed Defendants about FACTA, including its specific requirements concerning the truncation of credit and debit card numbers and prohibition on the printing of expiration dates, and Defendants' need to comply with same.

45. In addition, many companies such as VISA and MasterCard devised and implemented policies well before the operative date of FACTA's requirements, wherein such policies VISA, MasterCard and others required Defendants (and informed Defendants of the requirements) to truncate credit and debit card numbers and prevent the printing of expiration dates on receipts.

46. In addition, these companies also publically announced some of these requirements. For example, on March 6, 2003, VISA USA's CEO, Carl Pascarella, held a press conference on Capitol Hill with Senators Dianne Feinstein, Judd Gregg, Jon Corzine and Patrick Leahy, and publically announced Visa USA's new

truncation policy to protect consumers from identity theft. At the March 2003 press conference, Mr. Pascarella explained, as follows:

Today, I am proud to announce an additional measure to combat identity theft and protect consumers. **Our new receipt truncation policy will soon limit cardholder information on receipts to the last four digits of their accounts. The card's expiration date will be eliminated from receipts altogether.** This is an added security measure for consumers that doesn't require any action by the cardholder. We are proud to be the first payments brand to announce such a move to protect cardholders' identities by restricting access to their account information on receipts.

The first phase of this new policy goes into effect July 1, 2003 for all new terminals. I would like to add, however, that even before this policy goes into effect, **many merchants have already voluntarily begun truncating receipts, thanks to groundwork that we began together several years ago.**

Receipt truncation is good news for consumers, and bad news for identity thieves. Identity thieves thrive on discarded receipts and documents containing consumers' information such as payment account numbers, addresses, Social Security numbers, and more. Visa's new policy will protect consumers by limiting the information these thieves can access. (Emphasis added).

47. Moreover, the Government, through the Federal Trade Commission ("FTC"), provided notice of FACTA's requirements to businesses on no less than three separate occasions in 2007, reminding them of the requirement to truncate credit and debit card information on receipts. Defendants were informed of and knew about these notices from the FTC. In one such notice, entitled "FTC

Business Alert" "Slip Showing? Federal Law Requires All Businesses to Truncate Credit Card Information on Receipts," and dated May 2007, the FTC reminded businesses, among other things, of the following:

What's on the credit and debit card receipts you give your customers? The Federal Trade Commission (FTC), the nation's consumer protection agency, says it's time for companies to check their receipts and make sure they're complying with a law that's been in effect for all businesses since December 1, 2006.

According to the federal Fair and Accurate Credit Transaction Act (FACTA), the electronically printed credit and debit card receipts you give your customers must shorten — or truncate — the account information. **You may include no more than the last five digits of the card number**, and you must delete the card's expiration date. For example, a receipt that truncates the credit card number and deletes the expiration date could look like this:

ACCT:*****12345
EXP:****

Why is it important for businesses to make sure they're complying with this law? Credit card numbers on sales receipts are a "golden ticket" for fraudsters and identity thieves. Savvy businesses appreciate the importance of protecting their customers — and themselves — from credit card crime. (Emphasis added).

48. Defendants' violations of FACTA were not accidental oversights. The electronic printing of more than the last 5 digits of a credit or debit card number on a customer receipt does not occur by accident. Electronic receipt printing equipment must be intentionally programmed or otherwise intentionally configured

to print more than the last 5 digits of a credit or debit card number on a customer receipt.

49. Thus, despite knowing and being repeatedly informed about FACTA and the importance of truncating credit and debit card numbers and preventing the printing of expiration dates on receipts, and despite having had over three years to comply with FACTA's requirements, Defendants knowingly willfully, intentionally, and recklessly violated FACTA's requirements by, *inter alia*, printing more than the last 5 digits of the card number upon the receipts provided to the credit card and/or debit debit card cardholders with whom they transact business.

50. Many of Defendants' business peers and competitors brought their credit and debit card receipt printing processes in compliance with FACTA's requirements by, for example, programming their card machines and devices to prevent them from printing more than the last five digits of the card number and or the expiration date upon the receipts provided to the cardholders. Defendants could have readily done the same.

51. Instead, Defendants knowingly, willfully, intentionally, and recklessly disregarded FACTA's requirements and used cash registers and or other machines or devices that printed receipts in violation of FACTA.

52. Defendants knowingly, willfully, intentionally, and recklessly violated FACTA in conscious disregard of the rights of Plaintiff and the Class.

53. As explained above, Defendants have also harmed Plaintiff and the Class by exposing them to at least an increased risk of identity theft and credit and debit card fraud.

54. As a result of Defendants' willful violations of FACTA, Defendants are liable to Plaintiff and each member of the Class in the statutory damage amount of "not less than \$100 and not more than \$1,000" for each violation. 15 U.S.C. § 1681n.

PRAYER FOR RELIEF

55. WHEREFORE, Plaintiff prays for judgment and relief against Defendants as follows:

A. An order certifying the Class and appointing Plaintiff as the representative of the Class, and appointing counsel of record for Plaintiff as counsel for the Class;

B. An award to Plaintiff and the Class of statutory damages pursuant to 15 U.S.C. § 1681n for Defendants' willful violations (up to but not exceeding the fullest extent allowed under the Constitution of the United States);

C. An award to Plaintiff and the Class of punitive damages pursuant to 15 U.S.C. § 1681n (up to but not exceeding the fullest extent allowed under the Constitution of the United States);

D. Payment of costs of suit herein incurred pursuant to, *inter alia*, 15 U.S.C. § 1681n;

E. Payment of reasonable attorney's fees pursuant to, *inter alia*, 15 U.S.C. § 1681n;

F. For pre-judgment and post-judgment interest; and

G. For such other and further relief as the Court may deem proper.

JURY DEMAND

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

Respectfully submitted,

Date: February 9, 2018

/s/ Shaun Patrick O'Hara
Charles Austin Gower Jr.
Georgia Bar No. 303528
Shaun Patrick O'Hara
Georgia Bar No. 749503
CHARLES A. GOWER PC
1425 Wynnton Road
P.O. Box 5509

Columbus, GA 31906
Telephone: 706.324.5685
Facsimile: 706.322.2964
austin@cagower.com
shaun@cagower.com

Chant Yedalian (to apply *pro hac vice*)
California Bar No. 222325
CHANT & COMPANY
A Professional Law Corporation
1010 N. Central Ave.
Glendale, CA 91202
Telephone: 877.574.7100
Facsimile: 877.574.9411
chant@chant.mobi

**ATTORNEYS FOR PLAINTIFF AND
THE PUTATIVE CLASS**

EXHIBIT "1"



[\(http://www.ncl.ac.uk/\)](http://www.ncl.ac.uk/)

Press Office (/press/)

Six seconds to hack a credit card

Published on: 2 December 2016

New research reveals the ease with which criminals can hack an account without any of the card details.



“This sort of attack exploits two weaknesses that on their own are not too severe but when used together, present a serious risk to the whole payment system.”

Mohammed Ali, PhD student Newcastle University

Working out the card number, expiry date and security code of any Visa credit or debit card can take as little as six seconds and uses nothing more than guesswork, new research has shown.

Research published in the academic journal IEEE Security & Privacy (<https://www.computer.org/security-and-privacy/>), shows how the so-called Distributed Guessing Attack is able to circumvent all the security features put in place to protect online payments from fraud.

Exposing the flaws in the VISA payment system, the team from Newcastle University, UK, found neither the network nor the banks were able to detect attackers making multiple, invalid attempts to get payment card data.

By automatically and systematically generating different variations of the cards security data and firing it at multiple websites, within seconds hackers are able to get a 'hit' and verify all the necessary security data.

Investigators believe this guessing attack method is likely to have been used in the recent Tesco cyberattack which defrauded customers of £2.5m and which the Newcastle team describe as "frighteningly easy if you have a laptop and an internet connection."

And they say the risk is greatest at this time of year when so many of us are purchasing Christmas presents online.

Unlimited guesses

"This sort of attack exploits two weaknesses that on their own are not too severe but when used together, present a serious risk to the whole payment system," explains Mohammed Ali, a PhD student in Newcastle University's School of Computing Science (<http://www.ncl.ac.uk/computing/>) and lead author on the paper.

"Firstly, the current online payment system **does not detect multiple invalid payment requests from different websites**. This allows unlimited guesses on each card data field, using up to the allowed number of attempts - typically 10 or 20 guesses - on each website.

"Secondly, different websites ask for different variations in the card data fields to validate an online purchase. This means it's quite easy to build up the information and piece it together like a jigsaw.

"The unlimited guesses, when combined with the variations in the payment data fields make it **frighteningly easy for attackers to generate all the card details one field at a time**.

"Each generated card field can be used in succession to generate the next field and so on. If the hits are spread across enough websites then a positive response to each question can be received within two seconds – just like any online payment.

"So even starting with no details at all other than the first six digits – which tell you the bank and card type and so are the same for every card from a single provider – a hacker can obtain the three essential pieces of information to make an online purchase within as little as six seconds."

Distributed Guessing Attack

To obtain card details, the attack uses online payment websites to guess the data and the reply to the transaction will confirm whether or not the guess was right.

Different websites ask for different variations in the card data fields and these can be divided into three categories: Card Number + Expiry date (the absolute minimum); Card Number + Expiry date + CVV (Card security code); Card Number + Expiry date + CVV.

Case 1:18-cv-00622-MB-JFK Document 1-1 Filed 02/09/18 Page 4 of 8

Because the current online system does not detect multiple invalid payment requests on the same card from different websites, unlimited guesses can be made by distributing the guesses over many websites.

However, the team found it was only the VISA network that was vulnerable.

“MasterCard’s centralised network was able to detect the guessing attack after less than 10 attempts – even when those payments were distributed across multiple networks,” says Mohammed.

At the same time, because different online merchants ask for different information, it allows the guessing attack to obtain the information one field at a time.

Mohammed explains: “Most hackers will have got hold of valid card numbers as a starting point but even without that it’s relatively easy to generate variations of card numbers and automatically send them out across numerous websites to validate them.

“The next step is the expiry date. Banks typically issue cards that are valid for 60 months so guessing the date takes at most 60 attempts.

“The CVV is your last barrier and theoretically only the card holder has that piece of information – it isn’t stored anywhere else.

“But guessing this three-digit number takes fewer than 1,000 attempts. Spread this out over 1,000 websites and one will come back verified within a couple of seconds. And there you have it – all the data you need to hack the account.”

Protecting ourselves from fraud

An online payment – or “card not present” transaction – is dependent on the customer providing data that only the owner of the card could know.

But unless all merchants ask for the same information then, says the team, jigsaw identification across websites is simple.

So how can we keep our money safe?

“Sadly there’s no magic bullet,” says Newcastle University’s **Dr Martin Emms** (<http://www.ncl.ac.uk/computing/news/item/howtoprotectyourselfwhenusingacontactlesscardnewyorktimes.html>), co-author on the paper.

“But we can all take simple steps to minimise the impact if we do find ourselves the victim of a hack. For example, use just one card for online payments and keep the spending limit on that account as low as possible. If it’s a bank card then keep ready funds to a minimum and transfer over money as you need it.

“And be vigilant, check your statements and balance regularly and watch out for odd payments.

“However, the only sure way of not being hacked is to keep your money in the mattress and that’s not something I’d recommend!”

Publication Title: IEEE Security & Privacy

Article Title: **Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?**

(http://eprint.ncl.ac.uk/pub_details2.aspx?pub_id=230123)

Author(s): Ali, Mohammed Aamir; Arief, Budi; Emms, Martin; van Moorsel, Aad. Newcastle University, UK.

Share:

Latest News

Newcastle University students design new Kielder nature hide

Members of the public can now enjoy watching wildlife from a brand new nature hide at Kielder Water & Forest Park.

published on: 2 August 2017

(/press/news/2017/08/bakethinhide/)

Newcastle University celebrates Top 10 national ranking for sport

Another Top 10 BUCS ranking has cemented Newcastle as one of the best universities for sport in the UK.

published on: 1 August 2017

(/press/news/2017/08/bucstop10/)

Paediatric oncologist appointed Sir Bobby Robson Clinical Fellow

New specialist research roles, funded through the Sir Bobby Robson Foundation, are helping find more effective treatments for children's cancer in the North East.

published on: 26 July 2017

(/press/news/2017/07/sbrclinicalfellow/)

EXHIBIT "2"



Ali MA, Arief B, Emms M, van Moorsel A.

Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?

IEEE Security & Privacy 2017. In Press.

Copyright:

© 2017 IEEE. Personal use of this material is permitted.

Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

DOI link to article:

<http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013>

Date deposited:

01/12/2016

Does The Online Card Payment Landscape Unwittingly Facilitate Fraud?

Mohammed Aamir Ali, Budi Arief, Martin Emms, and Aad van Moorsel

Abstract—This article provides an extensive study of the current practice of online payment using credit and debit cards, and the intrinsic security challenges caused by the differences in how payment sites operate. We investigated the Alexa top-400 online merchants' payment sites, and realised that the current landscape facilitates a distributed guessing attack. This attack subverts the payment functionality from its intended purpose of validating card details, into helping the attackers to generate all security data fields required to make online transactions. We will show that this attack would not be practical if all payment sites performed the same security checks. As part of our responsible disclosure measure, we notified a selection of payment sites about our findings, and we report on their responses. We will discuss potential solutions to the problem and the practical difficulty to implement these, given the varying technical and business concerns of the involved parties.

Keywords—security; online payment; distributed attack; fraudulent transactions; survey; ethical disclosure.

I. INTRODUCTION

Cards are the *de facto* means of paying for online purchases. However, as the value of online sales has increased, so has the amount of online fraud. As an example, UK¹ online sales in 2014 was worth £45 billion, which represents a 16% growth between 2013 and 2014 [1]. In the same time period, the value of online fraud in the UK has increased by 33% to £217 million [1]. Online fraud is now the single largest category of card fraud in the UK, representing 45% of the total value of the fraud committed against UK credit and debit cards [2].

In this article, we present the online payment landscape in detail. In particular, we aim to highlight the different manners in which online payment is performed, and the varying security measures put in place by online merchants – from checking only the card number and the expiry date, to fully-fledged centralised bank security mechanisms such as 3D Secure [3][4][5]. There is a number of questions we would like to address: does the difference cause a security problem? if it does, how common is the problem and can it be exploited? how much damage can be done? and how could it be resolved in the future? To determine the extent of the problem, we survey the 'online payment landscape', creating a mapping of various merchant payment implementations.

We came to an important observation that the difference in security solutions of various websites introduces a practically exploitable vulnerability in the overall payment system. An attacker can exploit these differences to build a distributed guessing attack which generates usable card payment details (card number, expiry date, card verification value, and postal address) *one field at a time*. Each generated field can be used in succession to generate the next field by using a different merchant's website. Moreover, if individual merchants were trying to improve their security by adding more payment fields to be verified on their site, they potentially inadvertently weaken the whole system by creating an opportunity to guess the value of another field, as explained later in the article.

We demonstrate the practicability of exploiting the vulnerabilities with software that implements the distributed guessing attack. We will show that the potential impact of these vulnerabilities is substantial because the card details generated by this distributed attack can be used to transfer money from a victim's bank account to an anonymous recipient overseas using a financial services company such as the Western Union as a conduit.

The vulnerabilities described in this article apply to cards that do not enforce centralised checks across transactions from different sites. Our experiments were conducted using Visa and MasterCard only. Whereas MasterCard's centralised network detects the guessing attack after fewer than 10 attempts (even when those attempts were distributed across multiple websites), Visa's payment ecosystem does not prevent the attack (see Section VI.D). Because Visa is the most popular payment network in the world, the discovered vulnerabilities greatly affect the entire global online payments system.

We also carried out a responsible disclosure exercise with the payment sites affected by these vulnerabilities. Of the 342 vulnerable websites, we presented our findings to the top-36 of these sites (in terms of the severity of the vulnerabilities and the size of their customer base), monitored their responses, and analysed the changes these websites have implemented to deal with our disclosure. Several websites, including some of the largest and most popular websites in the world, changed their approach to online payment processing after our disclosure, as we will report later in this article. To protect the affected sites,

¹ Sales and fraud statistics from regions other than the UK are less reliable but indicate the same pattern.

we refrain from specifically revealing their names and their vulnerabilities.

Finally, we discuss potential solutions to the problem. We will see that the vulnerabilities are systemic and cannot be protected against in isolation by any individual online merchant or by the issuing bank through improving their own security policies. But first, let us look into how current online payment system operates.

II. OVERVIEW OF THE ONLINE PAYMENT SYSTEM

An online payment site uses a customer's existing credit or debit card to transfer funds from the customer's bank account into the merchant's bank account. For this to happen, the customer needs to provide their card information during checkout. These pieces of information are then passed to the card issuing bank, who will process the information further before authorising or rejecting the payment request. This process involves a number of parties, each with different responsibilities.

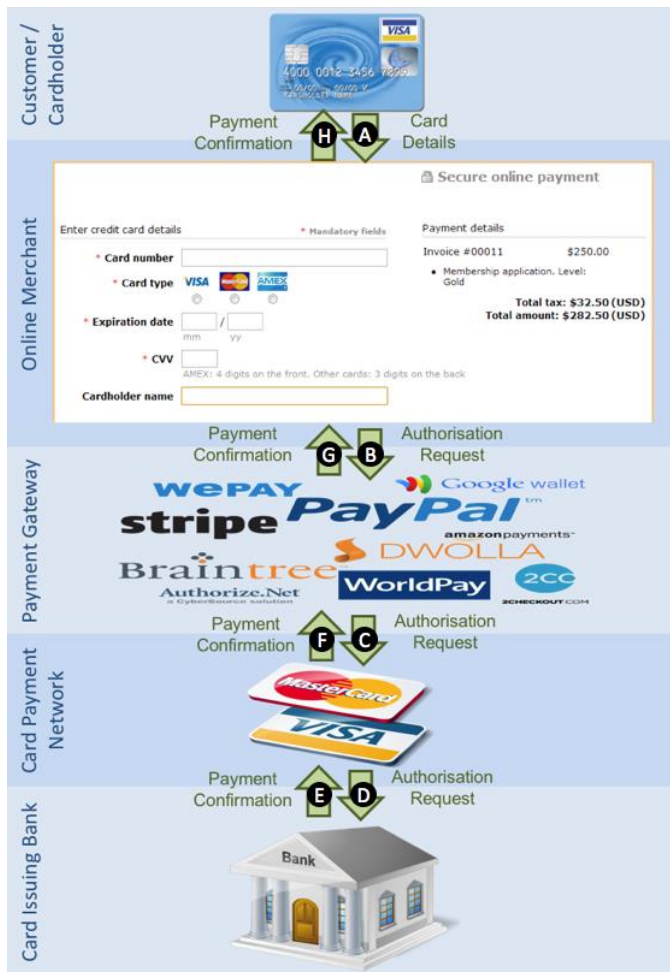


Fig. 1. Actions and parties in online payment.

A. Online Payment Process and Parties Involved

Fig. 1 illustrates the actions and parties involved in processing online payments. The process involves the customer/cardholder entering their payment card details on the

payment page of the online merchant's website (action **A** in Fig. 1). The merchant controls which data fields are used to authorise the payment.

The merchant then passes the card details to their chosen payment gateway, which provides a service of authorising and processing the merchant's payment request (action **B**). The payment gateway, on behalf of the merchant, can also implement additional security filters at this point (further details can be found in Section VI.C). The payment gateway then connects the merchant to the card payment network to request payment from the customer's bank account held at the card issuing bank. The payment networks (such as Visa and MasterCard) provide the link between payment gateways and the thousands of card issuing banks (actions **C** and **D**).

The card-issuer holds the customer's bank account and makes the approval of the payment (action **E**). The issuer maintains customer's card record file, which contains information such as account balance, customer name, full address, and other card details not visible to the rest of the payment network. In the final step, called a settlement, the card-issuing bank subsequently deposits the customer's money to the merchant's bank account (actions **F**, **G** and **H**).

B. Payment Card Data Fields

An online payment is a "card-not-present" credit or debit card transaction [6]. This implies the merchant cannot physically verify that the customer actually has the card. The security of online payment is therefore dependent upon the customer providing data that only the owner of the card could know.

The payment card industry has developed a Payment Card Industry Data Security Standard (PCI DSS) [7], which provides a comprehensive set of rules and controls for the secure handling and storage of sensitive card data. However, there is no requirement for the merchant to request all of the data fields during an online payment authorisation, nor is there a mandatory requirement for the merchant to implement any of the optional security filters. Five pieces of information are typically used when making an online payment:

- **Cardholder Name:** the account holder's name as printed on the card. We found that no website checks that a name entered is correct.
- **16-digit Card Number:** a unique identifier printed on the front of the card by the issuing bank. Referred to as the *Primary Account Number (PAN)*, it links the card to the customer's bank account.
- **Card Expiry Date:** printed or embossed on the front of the card. The expiry date and the PAN constitute the minimum set of card authentication data.
- **Card Verification Value (CVV2):** a 3-digit number printed on the reverse side of the card. It is meant to be known only to the person possessing the card. It should not be stored electronically anywhere in the payment ecosystem [7].
- **Cardholder Address:** not visible on the card but sometimes used for payment authorisation purposes. Address verification is performed only on the numerical values of the street/house and postcode fields; any alphabetical characters

are ignored. Different websites perform varying levels of verification on the address field's numerical digits, ranging from verifying just the numerical digits in the postcode (partial match), to the complete numerical digits in postcode plus the door number (full match) [8].

III. DISTRIBUTED GUESSING ATTACK

To obtain card details, one can use a web merchant's payment page to guess the data: the merchant's reply to a transaction attempt will state whether the guess was correct or not. The reason this attack works in practice is due to two weaknesses, each not too severe on its own, but when used together present a serious risk to the global payment system.

The first weakness is that in many settings, the current online payment system does not detect multiple invalid payment requests on the same card from different websites. Effectively, this implies that practically unlimited guesses can be made by distributing the guesses over many websites, even if individual websites limit the number of attempts.

Secondly, the attack scales well because different web merchants provide different fields, and therefore allow the guessing attack to obtain the desired card information one field at a time. To understand how essential the scaling issue is, we look at the differences in websites in some more detail. The data fields that web merchants use can be divided into three categories:

- 2 fields: PAN + Expiry date (the absolute minimum)
- 3 fields: PAN + Expiry date + CVV2
- 4 fields: PAN + Expiry date + CVV2 + Address

Starting with a valid card number (PAN), to guess the expiry date an attacker can utilise several merchants' websites that check only two fields: the card number and the expiry date. Once the expiry date is known, the attacker can use it along with the card number to guess the CVV2 information using another set of websites that check 3 fields (the card number, the expiry date, and the CVV2).

Guessing an expiry date takes at most 60 attempts (banks typically issue cards that are valid for up to 60 months), and subsequently, guessing the 3-digit CVV2 takes fewer than 1,000 attempts. Hence, expiry date and CVV2 are guaranteed to be obtained within $60 + 1,000 = 1,060$ guesses. If all merchants would use three fields and ask for expiry date as well as CVV2, then it may take as many as $60 \times 1,000 = 60,000$ attempts. The difference between 1,060 and 60,000 is the difference between a quick and practical attack, and a tedious, close to impractical attack.

For many purposes, knowing the PAN, expiry date and CVV2 is sufficient to use a card online, but for some purchases, an attacker would also need to obtain address information. To guess address information, the attacker needs to use websites that ask for 4 fields. The address field is used in a variety of manners, based on the *Address Verification System* (AVS), which validates the billing address provided by the customer against the address information stored by the card-issuing bank [6][8][9]. The process of getting cardholder's address for the countries that have a long postcode (more than 3 numerical

digits) is not as straightforward as getting the expiry date or CVV2 because first, the attacker will need to narrow down the possible postcodes of the cardholder's address. This can be done by querying the first six digits of a PAN through well-known online databases such as BinDb [10] and ExactBins [11], which will reveal the card's brand, issuing bank name, and card type. Once the issuing bank is known, the attacker can increase the probability of guessing the right postcode by assuming that the victim is likely to be registered with one of the branches nearby – this is particularly relevant if the attacker uses NFC skimming to obtain the PAN and expiry date in the first place (see Section IV.B). Now, the attacker just needs to start brute force guesses from a list of issuing bank postcodes for a particular city where the card details have been skimmed from.

IV. EXPERIMENTS

We implemented a set of software tools to carry out the distributed guessing attack, using the research team's own cards to verify that it is indeed possible and practical to obtain all the information of the card. Included are seven Visa cards with a spread of PAN, expiry date, and CVV2 values. We selected 400 Alexa [12] top rated commercial websites for our investigation. These include many global websites such as iTunes, Google, PayPal, and Amazon.

A. Software Tools

The software tools implemented for the experiments consist of a website bot and automated scripts written in Java Selenium browser automation framework [13]. All the experiments were run on Mozilla Firefox web browser. Fig. 2 shows a screenshot of the website bot, which was used to automate the process of guessing relevant card information. The bot cycles through the possible values for each field to find the correct information.

The screenshot displays a web application interface for a distributed guessing attack. It is organized into three main sections, each with a 'Log' column on the right.

- 1. Generate Random Card:** Includes a 'BIN' field (47) and a 'Last' field. A button labeled '1. Card Number' is present. The log shows 'Trying [redacted] for CVV: Attempts from: 1-11' and 'Please follow IDE Logs for results'.
- 2. Get Expiry Date:** Includes 'Card Number' (47), 'ExpMM' (02), 'ExpYY' (2016), and 'Website' (dropdown). A button labeled '2. Get Expiry Date' is present. The log shows 'Trying [redacted] for CVV: Attempts from: 12-22' and 'Please follow IDE Logs for results'.
- 3. Get CVV:** Includes 'Card Number' (47), 'ExpMM' (02), 'ExpYY' (2016), 'CVV: From' (056), 'CVV: To' (066), and 'Website' (dropdown). A button labeled '3. Get CVV' is present. The log shows 'Trying [redacted] for CVV: Attempts from: 34-44' and 'Please follow IDE Logs for results'.

Fig. 2. Screenshot of the website bot, farming CVV2 from multiple sites.

B. Obtaining Card Data

The PAN is the starting point for the generation of all of the other card data fields. There are at least two known methods of obtaining valid PANs. Criminals sell bulk lists of card details online. These lists are considered less valuable when they do not contain the CVV2; nevertheless, such a list could be used as a source of PANs from which the expiry date, CVV2 and address information can be generated. Another method is by exploiting the contactless feature common in recently issued payment

cards. NFC skimming [14] provides an attacker with the PAN, the expiry date and in some cases, the cardholder's name. It is also possible to generate PAN using the first six digits of a PAN and the Luhn's algorithm [15] and getting it verified. However, we did not take this approach because it is crossing the boundary of ethical research—we only used our own cards.

Once the PAN is known, an attempt to obtain the expiry date can commence. We note that sometimes the expiry date can be obtained at the same time as the PAN, for example by using the NFC skimming method described above. But if that is not possible, the bot can be used to systematically guess the expiry date of a given PAN on the websites that do not require CVV2 to be entered. The next step in card data generation involves getting the card's CVV2. To find the correct CVV2, the bot will simply need to cycle through the possible values starting from 001 until the payment website blocks further attempts. A handful of payment sites allowed unlimited attempts while most of the other payment sites allowed 5, 10 or even 50 attempts to enter a correct CVV2. In our scenario, we "farm out" the brute force guessing attack to tens or even hundreds of payment systems, which practically means we can carry out unlimited guesses. The final step generates the cardholder's address. An attacker can exploit the different variants of address verification system (discussed in Section III) to find the full address of the cardholder.

C. Transferring the Money

Once either two, three, or four fields of the card data have been obtained, the attacker can use them to purchase goods on a website. This is damaging enough for the owner of the card, but we looked at even more impactful attacks. Rather than buying online goods from an e-commerce website, we created an attack scenario that uses the card details to open a money transfer account, sends the money to an anonymous recipient abroad, where the money is picked up within minutes of issuing the transfer. The attacker needs to be able to clear the funds before the issuing bank reverses the payment and thwarts the attack. It is therefore desirable from the attacker's point of view that the funds are transferred to an account outside the country (because it is more time consuming and costly to reverse payment across countries) or be conducted through a wire transfer to an anonymous cash recipient by using services such as the Western Union.

In our experiment, the card information extracted using our bot was used to create a bogus account from which we transferred money to a recipient in India. Within minutes, we received a confirmation email for the order made, and our contact confirmed the pick-up of the money. The time it took from the process of creating an account to collecting the money at the destination was only 27 minutes, which is short enough to avoid the bank reversing the payment.

D. Results

Our results (detailed in Table I) show that the distributed guessing attack described in Section III is indeed practical and so a credible threat. We studied and tested the payment website of 389 of Alexa's most visited sites (we looked at the Alexa top-400 sites, but 11 of them did not reveal sufficient useful information for our experiment). As shown in Table I, 26 sites use only two fields for card payment and an attacker would use

these sites to guess the expiry date. 291 sites use three fields, which one can use for guessing the CVV2, and 25 sites use four fields, which allows one to guess the postcode of the address. Finally, of the 389 sites, 47 merchants (i.e. 12%) had implemented 3D Secure payments (these sites are impervious to the distributed guessing attack, see Section VI.B).

There is also a variation in the number of attempts allowed at each of these sites, ranging from 4, 5, 10, 20, 25, 50, or even unlimited. In Table I, the number of sites that allow certain number of guesses is shown in the rows, for each type of site (as represented in the columns). We see that most sites (276) allow between 6 and 10 attempts, but 6 sites set no limit to the number of attempts. There were two notable outliers to this observation in the top-10 highly popular websites, one of which allowed unlimited attempts to guess the CVV2, while the other required only the 16-digit card number plus the expiry date.

Our experiments successfully obtained the valid expiry date for each of our Visa test cards, without exception. We also managed to find valid CVV2 information for our Visa test cards, again without exception. We performed more than 11,000 CVV2 iterations using our bot and scripts, and our experiments confirmed that there is no centrally imposed limit on the number of CVV2 attempts when distributing guesses over multiple websites. The final step is to obtain the address information. Our tests performed more than 3,000 iterations on the group of websites that verify partial address (only postcode digits), to get numerical digits of the postcode. We extended our experiments and run instances of our bot on another set of payment sites (which verify the door number and the postcode digits) in order to get the full address of all our Visa test cards.

TABLE I. VARIATION IN PAYMENT SECURITY SETTINGS OF ONLINE PAYMENTS WEBSITES

Number of attempts allowed	Sites with 2 fields (guess expiry date)	Sites with 3 fields (guess CVV2)	Sites with 4 fields (guess address postcode)	Sites with 3D Secure (safe from attack)	Total
0 to 5	2	23	2	-	27
6 to 10	20	238	18	-	276
11 to 50	2	28	3	-	33
Unlimited	2	2	2	-	6
3D Secure	-	-	-	47	47
Total	26	291	25	47	389

These experiments have also shown that it is possible to run multiple bots at the same time on hundreds of payment sites without triggering any alarms in the payment system. Combining that knowledge with the fact that an online payment request typically gets authorised within 2 seconds makes the attack viable and scalable in real time. As an illustration, with the website bot configured cleverly to run on 30 sites, an attacker can obtain the correct information within 4 seconds.

V. RESPONSIBLE DISCLOSURE

Two weeks after we completed the distributed guessing attack experiments, we initiated an ethical/responsible disclosure exercise, notifying Visa and a selection of affected sites. Based on the number of fields that a website checks, we categorised them into three groups: expiry date, CVV2 and postcode. Since the total number of vulnerable websites was very high, we selected the 12 biggest players from each category (in terms of the highest number of users), taking the total number of notified websites to 36.

Once a suitable contact person or team for each website was found, we presented them with the disclosure information that featured the experiments we performed and the type of vulnerabilities on their site. We used our official work/university email address and this served as a means for these merchants to trace us back, so that they can verify our authenticity. This would also allow them to request more detailed and technical information about our experiments should they wish to find out more.

We recorded the responses received from these websites over the duration of four weeks after we disclosed the vulnerabilities to them. Altogether, we received 20 human responses from 10 websites and 18 websites came back to us with machine generated response mostly confirming the receipt of our notification. All of the human responses requested more technical details while some asked us to suggest solutions. Out of the 36 websites we contacted, eight never responded. When a web merchant requested more information, we offered them an initial draft of this article, which explained the experiments and the attack to help them understand the actual problem. We followed the disclosure policy requested by the websites and anonymised the affected sites in our article.

TABLE II. NATURE OF PATCHING ON THE NOTIFIED WEBSITES

Web site	Information Leak	Patching Behaviour				
		Adding Addr. field	Adding Delay filter	Adding velocity filter (PAN based)	Adding velocity filter (IP based)	Adding CAPTCHA
A	Exp. date	✓				
B	Exp. date	✓				
C	Exp. date		✓			
D	Exp. date		✓			
E	CVV2			✓		
F	CVV2				✓	
G	CVV2				✓	✓
H	CVV2				✓	✓

As a result of our disclosure process, eight of the 36 websites changed their online security settings but the other 28 websites remained unchanged four weeks after the disclosure. We call such changes ‘patches’ in what follows, and Table II illustrates the nature of the patching of the notified websites. Of the eight

websites that modified their approach (labelled A to H), four used two fields (labelled ‘Exp. Date’ in the ‘Information Leak’ column) and four used three fields (labelled ‘CVV2’).

In most cases, we learned about the patching behaviour through manual observations, but in two cases (*Website B* and *Website G*), the affected websites notified us about the changes they made. *Website A* and *Website B* patched their checkout system by adding an address verification field. However, this was not a good idea because it did not provide additional security, but instead opened up a new avenue for guessing as will be discussed at the end of this section.

Typically, an online payment request is authorised almost instantly (within 2 seconds). From our observation, we noticed that *Website C* and *Website D* (both with expiry date leak) had introduced additional delays to the payment authorisation processing times. They did it in a staggered manner: few attempts were processed instantly but after certain incorrect attempts had taken place, the time taken for payment confirmation were increased. In this manner, fewer attempts were available (at least practically speaking) to enter the right expiry date without setting a hard upper bound to the number of attempts.

We found that *Website E* (one of the Alexa top-10 websites in terms of the number of visitors) patched their checkout system by adding PAN velocity filters, reducing the number of attempts allowed (based on the PAN) from unlimited to 100 attempts within 24 hours. *Website F* followed a similar approach and added IP-based velocity filter to limit the number of attempts to get CVV2 from 50 to 10 in 24 hours. Initially, *Website G* and *Website H* added CAPTCHA on their checkout page, thus disrupting our bot from carrying out the attack. Our experiment protocol limited the interaction with the administrators of notified websites. Due to complex trade-offs that payment websites need to consider when deciding which fields and filters to use, our ethical disclosure protocol did not volunteer advice about what actions to take to deal with the vulnerabilities. However, in one situation we felt we needed to depart from the protocol, namely in the case of *Websites G* and *H*, who added a CAPTCHA. CAPTCHAs prevent automated attempts in getting the sensitive card information but may adversely affect the usability of those websites [16]. To help *Websites G* and *H* to better understand the implications of adding a CAPTCHA, we provided these two websites with more detailed information about the attacks. This resulted in the CAPTCHA being replaced with IP address velocity filters, which allowed five attempts per IP address in 24 hours (hence a mark in two cells in Table II for these websites).

The overall result of our study on the nature of patching on the notified websites revealed that the vast majority (78%) did not make a change. We do not know the reason behind this and further research will be needed to find the explanation. Of the eight that patched, the general approach taken by merchants is either to add a filter to make it more cumbersome to try many times (6 of 8 sites that patched added delay or velocity filters), or to add a field (*Website A* and *Website B*). Perhaps surprisingly, none of the sites reacted by simply putting a hard limit on the number of allowed attempts. The effect of these patching behaviours is not so obvious. As we already pointed

out, the sensible measure of limiting the number of attempts will not stop the guessing attack if it is not done on all websites. Furthermore, adding a card validation field may be a reasonable idea for a site for various reasons, but inadvertently may even weaken the protection against the guessing attack of the payment system as a whole. After all, the added field may be a welcome opportunity to attempt guesses on this added card detail.

VI. THE CHALLENGES IN SOLVING THE PROBLEM

Improving the security of the online payment system is a complicated challenge for a variety of reasons. One could argue that payment card security mechanisms are bound to remain unsatisfactory since they have not been designed for distributed operation over the distributed Internet. Many of the solutions, such as 3D Secure can be seen as afterthoughts, and they struggle to gain widespread adoption. Any suggested improvement or solution faces the challenge that the online landscape contains many players that all have their own – at times competing – incentives for or reasons against change. Any solution would have to combine technical concerns with financial and business operational concerns, and its adoption will depend on legal and economic dynamics. We explore and discuss these issues from the perspectives of the five parties shown in Fig. 1.

A. Customer / Cardholder

Since the distributed guessing attack described in this article uses merchant websites and card payment network to get all the card details, there is not much a cardholder can do to prevent it. At the same time, the cardholder is severely impacted by the attack: money may be lost, cards may have to be blocked, and the result is a waste of time and effort and a decreased sense of security. Arguably, it would be beneficial for cardholders if they could get organised as a group, or would have representatives in various bodies, to put pressure on the other stakeholders. As an individual, cardholders could ‘vote with their feet’ and select cards from card payment networks that are not exposed to the distributed guessing attack. At the moment, the payment system is too complex and non-transparent to expect customers to be able to make such choices.

B. Online Merchant

On their own, a merchant can do very little to prevent distributed guessing attacks. All merchants would have to agree or be forced to use the same number of fields so that the guessing attack cannot be staged as explained in Section III.

At the same time, a merchant can avoid being exploited in the attack either by only using cards that use a payment network that is not vulnerable from the attack, or by using 3D Secure technologies recommended by the payment card industries [7], such as the American Express ‘SafeKey’ [3], ‘Verified by Visa’ [4] and MasterCard ‘SecureCode’ [5]. If 3D Secure is implemented, the card issuing bank is responsible for authenticating a cardholder before authorising the payment and it monitors the frequency of transactions and the total value of purchases for each card or bank account. The system will initiate additional security checks such as IP address and/or request an additional password if the frequency or value of the transactions appears to be unusual. Our experiments confirmed that 3D Secure payments are protected from the distributed guessing

attack described in this article since the issuing bank has visibility of all transaction requests directed at a single card, even if those requests are distributed across many websites.

From the perspective of the merchant, 3D Secure has several drawbacks, and these are reflected in that only 47 merchants in the Alexa top-400 have elected to implement 3D Secure. First, the proportion of the customers who do not complete the transaction can be high when the customer encounters the 3D Secure login screen: up to 43% in the United States and 55% in China [17]. Second, there are additional costs associated with implementing 3D Secure.

We reiterate that from the whole payment system’s perspective, we would need a very high adoption rate of 3D Secure technology to prevent the distributed attack, because the attack would still work as long as there are sufficient vulnerable websites not using 3D Secure.

C. Payment Gateway

There are many payment gateways, which charge web merchants different rates depending on the number of fields and filters they ask to check and utilise. One cannot expect all of these gateways to be able to coordinate sufficiently to prevent the distributed guessing attack. Nevertheless, payment gateways can provide advanced features to their merchants, and these features should at least make it more difficult to exploit a website for the attack. Most importantly, gateways may use IP address velocity filters [6][8][9], which are implemented to detect repeated invalid attempts made within a certain time span from the same IP address. But with no coordination between different gateways, these velocity filters can easily be circumvented just by switching to a website that uses a different payment gateway.

D. Card Payment Network

Responsibility for authorising online payment requests ultimately resides with the bank which issued the credit / debit card. However, our experiments have shown that distributed guessing attack described in the paper only works on Visa cards, independent of which bank issued the card. When the attack is applied to a MasterCard, the distributed attack is detected. This suggests that the payment networks have the capability to detect and prevent a distributed attack where the network is globally integrated [18].

The most obvious defence against the distributed guessing attack would be at the level of the card payment network. However, we are not in a position to know whether payment network providers could modify their network infrastructure to detect payment requests from multiple, globally spread payment gateways, looking for suspicious activities on a single card distributed across multiple merchant websites.

E. Card Issuing Banks

The bank comes into play at the final stage of the payment process, to approve the transfer of funds, but it would not be party to each individual guess (unless 3D Secure is used). Banks play an important role in limiting the damage that can be done if attackers get hold of card information. Many issuing banks are now running intelligent fraud detection systems which detect transactions which are outside their customer’s normal spending

habits [6]. The issuing bank then has the option to block the payment, or ask the customer for confirmation, or accept the payment taking a calculated risk that a transaction may be found to be fraudulent later. A complicated set of considerations comes to the fore in the bank's decisions, from ease of use to financial risks. However, one would expect that if they so desire, banks could have considerable influence on the payment gateways and card payment networks in protecting against the distributed guessing attack.

VII. CONCLUSION

In this paper, we studied 400 of the most popular e-commerce websites and surveyed their web payment interface, identifying that different websites present different sets of fields to identify the cardholder. It turns out that this disparity between different websites inadvertently creates conditions for a scalable distributed guessing attack. By conducting a guessing attack one field at the time – using a set of appropriate websites at each stage – the attack becomes practical. With the obtained data, the attacker can make purchases or transfer funds, as we have demonstrated.

We showed that the attack works if the card payment network is not able to relate card activities from different websites. Fundamentally, much of the problem with card payment stems from the fact that the identity of the payer needs to be established in the 'card-not-present' mode. This is inherently problematic since it is at odds with the original use of cards (where the card and cardholder are present at the moment of purchase). It also implies that, for instance, Chip-and-PIN is not available to establish the identity of the payer. This is exacerbated by the fact that the Internet facilitates distribution of guesses for data fields over many merchant sites.

To prevent the attack, either standardisation or centralisation can be pursued (some card payment networks already provide this). Standardisation would imply that all merchants need to offer the same payment interface, that is, the same number of fields. Then the attack does not scale anymore. Centralisation can be achieved by payment gateways or card payment networks possessing a full view over all payment attempts associated with its network. Neither standardisation nor centralisation naturally fit the flexibility and freedom of choice one associates with the Internet or successful commercial activity, but they will provide the required protection. It is up to the various stakeholders to determine the case for and timing of such solutions.

ACKNOWLEDGEMENTS

This material is based in part on research supported by the UK EPSRC EP/K006568 Research Institute for Science of Security—Choice Architecture for Information Security.

REFERENCES

- [1] UK Office for National Statistics, "Retail Sales, February 2015," http://www.ons.gov.uk/ons/dcp171778_399119.pdf, 26 March 2015, Accessed: 13 May 2016.
- [2] Financial Fraud Action UK, "Fraud the Facts 2015: The definitive overview of payment industry fraud and measures to prevent it," London: UK Cards Association, 2015, www.financialfraudaction.org.uk/download.asp?file=2979, Accessed: 13 May 2016.
- [3] American Express SafeKey, "Product Capability Guide," https://network.americanexpress.com/en/globalnetwork/Images/SafeKey/ProductCapabilityGuide_2014.pdf, Accessed: 04 Mar 2016.
- [4] Visa, "3D Secure System Overview," http://www.visanet.com.pe/verified/demovisanet-web/resources/3DS_70015-01_System_Overview_external_v1.0.3.pdf, 2001, Accessed: 12 May 2016.
- [5] MasterCard, "MasterCard Secure Code, "Merchant Implementation Guide," https://www.mastercard.us/content/dam/mccom/en-us/documents/SMI_Manual.pdf, 2014, Accessed: 13 May 2016.
- [6] Visa, "Card Acceptance Guidelines for Visa Merchants," <http://usa.visa.com/download/merchants/card-acceptance-guidelines-for-visa-merchants.pdf>, 2014, Accessed: 13 May 2016.
- [7] Payment Card Industry, "PCI DSS Applicability in an EMV Environment," https://www.pcisecuritystandards.org/documents/pci_dss_emv.pdf, 2010, Accessed: 13 May 2016.
- [8] PayPal, "Gateway Developer Guide and Reference," https://www.paypalobjects.com/webstatic/en_US/developer/docs/pdf/payflowgateway_guide.pdf, 2014, Accessed: 11 Mar 2016.
- [9] MasterCard, "Transaction Processing Rules," http://www.mastercard.com/us/merchant/pdf/TPR-Entire_Manual_public.pdf, 2014, Accessed: 13 May 2016.
- [10] BinDb, "Bank Identification Numbers Database - Credit Card Bin Lookup," <https://www.bindb.com/structure.html>, Accessed: 13 May 2016.
- [11] ExactBins, "Exact BIN Database," <https://www.exactbins.com/features>, Accessed: 13 May 2016.
- [12] Alexa, "Alexa Top Shopping Sites," <http://www.alexa.com/topsites/category/Top/Shopping>, Accessed: 13 May 2016.
- [13] SeleniumHQ, "Selenium framework documentation," <http://docs.seleniumhq.org/docs/>, Accessed: 17 May 2016.
- [14] M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel, "Harvesting High-Value Foreign Currency Transactions from EMV Contactless Credit Cards Without the PIN," In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS'14), ACM, 2014, pp. 716-726.
- [15] Symantec, "Validating a Credit Card Number using Luhn's Algorithm," https://support.symantec.com/en_US/article.TECH221769.html [Accessed: 09 May 2016]
- [16] A. El Ahmad, J. Yan and W. Ng, "CAPTCHA Design: Color, Usability, and Security", *IEEE Internet Computing*, vol. 16, no. 2, pp. 44-51, 2012.
- [17] Adyen, "Analysis Reveals Worldwide Impact of 3D Secure on Transaction Conversion Rates," <https://www.adyen.com/home/about-adyen/press-releases/2014/3d-secure-worldwide-impact-conversion>, 2014, Accessed: 13 May 2016.
- [18] MasterCard, "The MasterCard Network Advantage," <http://newsroom.mastercard.com/wp-content/uploads/2011/09/MasterCard-Network-Advantage.pdf>, Accessed: 12 May 2016

Mohammed Aamir Ali is currently a Ph.D. research student at the centre of cybercrime and computer security at Newcastle University, UK. His research centres around exploiting the potential vulnerabilities in the payment eco-system (i.e. NFC mobile payments, payment applications and online payments). Understanding the insidious tactics targeting the world of cyber systems gives Mohammed an in-depth insight into the methods and psychology of attackers. He has ongoing research which involves landscaping the developments and security challenges in the ecommerce payment systems. Contact him at m.a.ali2@ncl.ac.uk

Budi Arief is a Lecturer in the School of Computing at the University of Kent, England. His research interests are in

cybercrime, the security and dependability of computer-based systems, cyber security education, and the Internet of Things, with a strong overarching element of interdisciplinary research. He obtained his B.Sc. in Computing Science (First Class) and Ph.D. in Computing Science, both from Newcastle University, England. Prior to joining the University of Kent, Budi was a Senior Research Associate in the School of Computing Science at Newcastle University, England. Contact him at b.ariief@kent.ac.uk

Martin Emms is a cyber security researcher at Newcastle University focusing on the security impacts of new payment technologies, user authentication using ubiquitous and IoT technologies and related security issues caused by unintentional privacy leakage. Martin's work is enhanced by his industry

experience; working as a solutions architect in payments and as a systems designer of safety critical embedded control systems for MoD, satellite comms, nuclear power and transport.

Aad van Moorsel is Professor and Head of School at the School of Computing Science in Newcastle University. His research interests are in cyber security and cybercrime, with an emphasis on decision making, quantification and risk management. He received a PhD in computer science from the University of Twente, The Netherlands. Contact him at ataad.vanmoorsel@ncl.ac.uk.

EXHIBIT "3"

PETER D. KEISLER
Assistant Attorney General
Civil Division
United States Department of Justice

EUGENE M. THIROLF
Director
Office of Consumer Litigation

ALAN J. PHELPS
D.C. Bar No. 475938
Trial Attorney
Office of Consumer Litigation
United States Department of Justice
1331 Pennsylvania Ave. NW, Suite 950N
Washington, DC 20004
Tel: 202-307-6154
Fax: 202-514-8742
E-mail: alan.phelps@usdoj.gov

Attorneys for the United States

UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA

HASMIK JASMINE PAPAZIAN,	)	No. CV 07-1479 GPS (RZx)
Plaintiff,	)	<u>BRIEF OF THE UNITED STATES</u>
v.	)	<u>IN SUPPORT OF 15 U.S.C.</u>
	)	<u>§ 1681c(g)</u>
BURBERRY LIMITED, et al.,	)	
Defendants.	)	Honorable George P. Schiavelli

TABLE OF CONTENTS

INTRODUCTION	4
ARGUMENT	4
A. <u>The requirements of § 1681c(g) are clear</u>	5
B. <u>Section 1681c(g) does not violate the First Amendment</u>	7
CONCLUSION	21

TABLE OF AUTHORITIES

<u>44 Liquormart, Inc. v. Rhode Island</u> , 517 U.S. 484 (1996)	8
<u>Aeschbacher v. California Pizza Kitchen</u> , 2007 WL 1500853 (C.D. Cal. Apr. 3, 2007)	7
<u>Arcilla v. Adidas Promotional Retail Operations, Inc.</u> , 488 F. Supp.2d 965, 2007 WL 1498334 (C.D. Cal. May 4, 2007)	7
<u>Big Bear Super Market No.3 v. INS</u> , 913 F.2d 754 (9th Cir. 1990)	6
<u>Bolger v. Youngs Drug Product Corp.</u> , 463 U.S. 60 (1983)	11
<u>California Teachers Ass'n v. Bd. of Educ.</u> , 271 F.3d 1141 (9th Cir. 2001)	6
<u>Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.</u> , 447 U.S. 557 (1980)	11-13
<u>City of Dallas v. Stanglin</u> , 490 U.S. 19 (1989)	9
<u>Clark v. Cmty. for Creative Non-Violence</u> , 468 U.S. 288, 293 n. 5 (1984)	10
<u>Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.</u> , 472 U.S. 749 (1985)	10
<u>Greater New Orleans Broad. Ass'n v. United States</u> , 527 U.S. 173 (1999)	12, 13
<u>Hill v. Colorado</u> , 530 U.S. 703 (2000)	5
<u>Hurley v. Irish-Am. Gay, Lesbian & Bisexual Group</u> , 515 U.S. 557, 569-70 (1995)	9
<u>Lopez v. Gymboree Corp.</u> , 2007 WL 1690886 (N.D. Cal., June 9, 2007)	7
<u>Lorillard Tobacco v. Reilly</u> , 533 U.S. 525 (2001)	12, 13

1	<u>Pirian v. In-N-Out Burgers</u> , 2007 WL 1040864 (C.D. Cal. Apr. 5,	
2	2007)	7
3	<u>Rumsfeld v. F.A.I.R.</u> , 547 U.S. 47, 126 S.Ct. 1297 (2006) . . .	9
4	<u>Soualian v. Int'l Coffee & Tea LLC</u> , Case No. CV 07-502-RGK (C.D.	
5	Cal., June 11, 2007)	4
6	<u>Spence v. Washington</u> , 418 U.S. 405, 410-11 (1974)	9
7	<u>Spikings v. Cost Plus, Inc.</u> , Case No. CV 06-8125-JFW (C.D. Cal.	
8	May 25, 2007)	4
9	<u>Texas v. Johnson</u> , 491 U.S. 397 (1989)	9
10	<u>Three Affiliated Tribes of Fort Berthold Reservation v. Wold</u>	
11	<u>Engineering, P. C.</u> , 467 U.S. 138 (1984)	4
12	<u>Trans Union v. FTC</u> , 245 F.3d 809 (D.C. Cir. 2001) . . .	8, 12-13
13	<u>Trans Union v. FTC</u> , 267 F.3d 1138 (D.C. Cir. 2001)	8, 20
14	<u>Turner Broad. System, Inc. v. FCC</u> , 520 U.S. 180, 217-18 (1997)	20
15	<u>United Reporting Pub. Corp. v. California Highway Patrol</u> , 146	
16	F.3d 1133 (9th Cir. 1998)	11
17	<u>United States v. Powell</u> , 423 U.S. 87 (1975)	6
18	<u>Universal City Studios, Inc. v. Corely</u> , 273 F.3d 429 (2d Cir.	
19	2001)	8
20	<u>Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.</u> ,	
21	455 U.S. 489 (1982)	6
22	<u>Villegas v. City of Gilroy</u> , 484 F.3d 1136 (9th Cir. 2007) . . .	9
23	<u>Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer</u>	
24	<u>Council, Inc.</u> , 425 U.S. 748 (1976)	8

INTRODUCTION

Pursuant to 28 U.S.C. § 2403, the United States of America ("United States") hereby submits this brief in defense of Section 113 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") (codified at 15 U.S.C. § 1681c(g)) and against the constitutional challenges presented by Defendant Burberry Limited in the Counterclaim included with Defendants' Answer (Dkt. #10). Section 1681c(g) is neither impermissibly vague nor does it infringe on any First Amendment right. The United States respectfully requests that the Court find § 1681c(g) constitutional.

ARGUMENT

As an initial matter, the government understands that Plaintiff's motion for class certification also is pending before this Court. The government does not intervene to take a stand on this issue, but notes that at least two courts in cases exactly like this one ruled against class certification. See Soualian v. Int'l Coffee & Tea LLC, Case No. CV 07-502-RGK (C.D. Cal., June 11, 2007) (available at 2007 U.S. Dist. LEXIS 44208); Spikings v. Cost Plus, Inc., Case No. CV 06-8125-JFW (C.D. Cal. May 25, 2007) (available at 2007 U.S. Dist. LEXIS 44214). Were this Court to also find against class certification, the case likely would be resolved without the necessity of determining the constitutional questions raised by Defendant. Therefore, the Court need not reach the constitutional issues at this time, depending on the outcome of the class certification motion. See Three Affiliated Tribes of Fort Berthold Reservation v. Wold Engineering, P. C., 467 U.S. 138, 157 (1984) ("It is a fundamental rule of judicial

1 restraint . . . that this Court will not reach constitutional
2 questions in advance of the necessity of deciding them.").
3 Should the Court determine that resolution of the constitutional
4 questions is presently necessary, however, case law provides
5 ready answers.

6 **A. The requirements of § 1681c(g) are clear**

7 Section 1681c(g) reads, in relevant part, as follows:

8 (g) Truncation of credit card and debit card numbers.

9
10 (1) In general. Except as otherwise provided
11 in this subsection, no person that accepts
12 credit cards or debit cards for the
13 transaction of business shall print more than
14 the last 5 digits of the card number or the
15 expiration date upon any receipt provided to
16 the cardholder at the point of the sale or
17 transaction.

14 15 U.S.C. § 1681c.

15 Defendant asserts that § 1681c(g) is impermissibly vague
16 because it does not specify whether retailers must truncate card
17 numbers *and also* delete expiration dates. Defendant claims that
18 the statute can reasonably be read to allow printing of a card
19 expiration date so long as the card number itself is truncated.
20 Such a reading ignores the plain language and purpose of the
21 provision. The statute as written does not offend due process
22 concerns.

23 A statute is unconstitutionally vague only if (1) "it fails
24 to provide people of ordinary intelligence a reasonable
25 opportunity to understand what conduct it prohibits" or (2) "it
26 authorizes or encourages arbitrary and discriminatory
27 enforcement." Hill v. Colorado, 530 U.S. 703, 732 (2000). This
28 requirement of a "reasonable" degree of clarity does not mean

1 Congress must use the most precise language conceivable. "The
2 fact that Congress might, without difficulty, have chosen clearer
3 and more precise language equally capable of achieving the end
4 which it sought does not mean that the statute which it in fact
5 drafted is unconstitutionally vague." United States v. Powell,
6 423 U.S. 87, 94 (1975) (quotation omitted).

7 Furthermore, as the Supreme Court has emphasized, "economic
8 regulation is subject to a less strict vagueness test [than
9 criminal statutes] because its subject matter is often more
10 narrow, and because businesses, which face economic demands to
11 plan behavior carefully, can be expected to consult relevant
12 legislation in advance of action." Village of Hoffman Estates v.
13 Flipside, Hoffman Estates, Inc., 455 U.S. 489, 498 (1982)
14 (footnote omitted); see also Big Bear Super Market No. 3 v. INS,
15 913 F.2d 754, 757 (9th Cir. 1990) ("when the statute regulates
16 the conduct of businesses . . . the vagueness test is relaxed,
17 because businesses have a greater ability to determine the
18 meaning of legislation in advance of their conduct than do
19 individuals.").

20 Vagueness concerns are more acute where a statute implicates
21 First Amendment rights. See Hoffman Estates, 455 U.S. at 499.
22 As set out below, the statute at issue does not restrict actual
23 speech protected by the First Amendment. Even if § 1681c(g)
24 applied to true expression, however, "perfect clarity is not
25 required even when a law regulates protected speech." California
26 Teachers Ass'n v. Bd. of Educ., 271 F.3d 1141, 1150 (9th Cir.
27 2001) (citing Ward v. Rock Against Racism, 491 U.S. 781, 794
28 (1989)). "[E]ven when a law implicates First Amendment rights,

1 the constitution must tolerate a certain amount of vagueness.”
2 Id. at 1151.

3 Section 1681c(g) easily passes muster under either vagueness
4 test because no reasonable person would read the statute in any
5 way other than prohibiting the printing on receipts of both
6 expiration dates and full card numbers. Read in the unreasonable
7 manner Defendant suggests, § 1681c(g) would allow retailers to
8 print full credit/debit card numbers so long as they did not
9 print the expiration date. Def.’s Mem. in Opp’n. to Pl.’s Mot.
10 to Dismiss, Dkt. # 21 (“Def.’s Br.”) at 4. Congress could not
11 have intended that absurd result. Indeed, at least four courts
12 have recently found, in the context of motions to dismiss brought
13 in cases mirroring the present action, that § 1681c(g) clearly
14 prohibits printing expiration dates. See Lopez v. Gymboree
15 Corp., 2007 WL 1690886, *3 (N.D. Cal., June 9, 2007); Arcilla v.
16 Adidas Promotional Retail Operations, Inc., 488 F. Supp.2d 965,
17 2007 WL 1498334, *3-5 (C.D. Cal. May 4, 2007); Pirian v. In-N-Out
18 Burgers, 2007 WL 1040864, *3 (C.D. Cal. Apr. 5, 2007);
19 Aeschbacher v. California Pizza Kitchen, 2007 WL 1500853, *3
20 (C.D. Cal. Apr. 3, 2007). Those courts were correct; the
21 argument advanced by Defendant has no merit.

22 **B. Section 1681c(g) does not violate the First Amendment**

23 Defendant’s First Amendment claim is similarly unconvincing.
24 First, it is highly questionable whether Defendant’s procedure of
25 copying card expiration dates and numbers to cash register
26 receipts constitutes speech at all. Second, even if the act of
27 transferring expiration dates to paper involves expressive
28

1 speech, the government's restriction on that speech is extremely
2 limited, reasonable, and constitutional.

3 Accepting a credit/debit card from a customer, copying the
4 card number or expiration date onto a receipt, and immediately
5 handing the card with receipt back to the customer is a rote act
6 devoid of expression and not "speech" covered by the First
7 Amendment. Defendant attempts to liken printing expiration dates
8 to commercial advertisements, instructions, or computer code.
9 Def.'s Br. at 8-9. While it is true that dry facts in
10 advertisements or instructions such as computer code can
11 constitute speech, that is not the situation here. All of the
12 cases Defendant cites involve statements laden with actual
13 information flowing from one party to another. See 44
14 Liquormart, Inc. v. Rhode Island, 517 U.S. 484 (1996) (liquor
15 store advertisements); Virginia State Bd. of Pharmacy v. Virginia
16 Citizens Consumer Council, Inc., 425 U.S. 748 (1976) (pharmacy
17 drug prices); Universal City Studios, Inc. v. Corely, 273 F.3d
18 429 (2d Cir. 2001) (computer code). Defendant's actions involve
19 no such expression of information; rather, the "speech" at issue
20 is more akin to the act of putting a credit card on a photocopy
21 machine and pressing the button.¹ The fact that Defendant's
22 conduct results in a printed date does not, by itself, implicate
23 the First Amendment. "[I]t has never been deemed an abridgment
24

25 ¹ As discussed below, courts have applied commercial speech
26 analysis in the context of other FCRA provisions. See Trans
27 Union v. FTC, 245 F.3d 809 (D.C. Cir. 2001); Trans Union v. FTC,
28 267 F.3d 1138 (D.C. Cir. 2001). In these cases, however, the
communications at issue involved far more than simply copying a
date from a card to a piece of paper. Rather, these cases
concerned the sale of mailing lists containing contact
information for consumers who met specific criteria.

1 of freedom of speech or press to make a course of conduct illegal
2 merely because the conduct was in part initiated, evidenced, or
3 carried out by means of language, either spoken, written, or
4 printed.” Rumsfeld v. Forum for Academic and Institutional
5 Rights, Inc., 547 U.S. 47, 126 S.Ct. 1297, 1308 (2006) (quotation
6 omitted).

7 Conduct can constitute speech, but only if it involves
8 expression. For good reason, not all conduct qualifies for First
9 Amendment protection. “It is possible to find some kernel of
10 expression in almost every activity a person undertakes – for
11 example, walking down the street, or meeting one’s friends at a
12 shopping mall – but such a kernel is not sufficient to bring the
13 activity within the protection of the First Amendment.” City of
14 Dallas v. Stanglin, 490 U.S. 19, 25-26 (1989) (law imposing age
15 limits on dance halls did not violate First Amendment freedom of
16 association). Communicative, constitutionally protected conduct
17 requires an intent to convey a particularized message that is
18 likely to be understood by those viewing it. See Spence v.
19 Washington, 418 U.S. 405, 410-11 (1974) (flying flag upside down
20 found expressive); see also Hurley v. Irish-Am. Gay, Lesbian &
21 Bisexual Group, 515 U.S. 557, 569-70 (1995) (discussing instances
22 in which the Supreme Court has found conduct to be inherently
23 communicative); Texas v. Johnson, 491 U.S. 397, 404 (1989)
24 (burning of flag found expressive); Villegas v. City of Gilroy,
25 484 F.3d 1136, 1139-41 (9th Cir. 2007) (wearing of vests with
26 skull insignia signifying no particular message found not
27 expressive). Furthermore, it is the duty of the party seeking to
28 engage in allegedly expressive conduct to demonstrate that the

1 First Amendment applies to that conduct. Clark v. Cmty. for
2 Creative Non-Violence, 468 U.S. 288, 293 n. 5 (1984) ("Although
3 it is common to place the burden upon the Government to justify
4 impingements on First Amendment interests, it is the obligation
5 of the person desiring to engage in assertedly expressive conduct
6 to demonstrate that the First Amendment even applies.").

7 Defendant offers no plausible argument that copying a date
8 already in the possession of a customer from one place to another
9 is an inherently expressive activity. It fact, such an action
10 communicates nothing in particular.

11 Even if Defendant could make a case that copying a date from
12 plastic to paper constitutes actual expressive speech, it would
13 be considered, at best, commercial speech. See Trans Union v.
14 FTC, 295 F.3d 42, 52-53 (D.C. Cir. 2002) (upholding a different
15 section of the FCRA and analyzing it under the commercial speech
16 doctrine). The Supreme Court has "long recognized that not all
17 speech is of equal First Amendment importance. It is speech on
18 matters of public concern that is at the heart of the First
19 Amendment's protection." Dun & Bradstreet, Inc. v. Greenmoss
20 Builders, Inc., 472 U.S. 749, 758-59 (1985) (quotations omitted).
21 In particular, "[commercial speech] may be regulated in ways that
22 might be impermissible in the realm of noncommercial expression."
23 Id. at 759 n.5 (citations omitted).

24 Defendant contends that because expiration dates are not
25 advertisements and do not refer to specific products, they cannot
26 be considered commercial speech. Def.'s Br. at 7, n.4.
27 Therefore, Defendant claims, printing expiration dates on
28 receipts actually deserves *greater* First Amendment scrutiny than

1 advertisements. Id. Defendant relies for this proposition on
2 the discussion of commercial speech in Bolger v. Youngs Drug
3 Product Corp., 463 U.S. 60 (1983), which found that such speech
4 often constitutes advertising in some form, references a
5 particular product, and is motivated by economic considerations.
6 Bolger, 463 U.S. 67-68.

7 Contrary to Defendant's argument, commercial speech is not
8 limited to advertisements for specific products, under Bolger or
9 any other case. As the Ninth Circuit has held, whether something
10 constitutes advertising "is the beginning of our inquiry . . .
11 not the end." United Reporting Pub. Corp. v. California Highway
12 Patrol, 146 F.3d 1133, 1137 (9th Cir. 1998) (rev'd. on other
13 grounds, Los Angeles Police Dept. v. United Reporting Pub. Corp.,
14 528 U.S. 32 (1999)). The Bolger Court itself explicitly stated
15 that commercial speech does not require "each of the
16 characteristics present in this case." Bolger, 463 U.S. at 67
17 n.14. In the seminal Central Hudson case, decided just a few
18 years prior to Bolger, the Supreme Court noted that commercial
19 speech can include any "expression related solely to the economic
20 interests of the speaker and its audience." Central Hudson Gas &
21 Electric Corp. v. Public Service Comm'n of New York, 447 U.S.
22 557, 561 (1980).

23 The Central Hudson definition is far more broad than the one
24 Defendant attempts to impose through its misreading of Bolger.
25 It covers the "speech" at issue, which, even as Defendant
26 describes it, does nothing more than confirm details of a
27 private, commercial transaction. See Def.'s Answer and
28 Counterclaim (Dkt. #10) ¶ 40 (printing of expiration date meant

1 to "confirm to [Defendant's] customers that a transaction has
2 been appropriately charged."). Such a communication relates only
3 to the economic interests of the merchant and the consumer. It
4 does not touch on any matter of public concern. It constitutes,
5 if anything, commercial speech.

6 Under Central Hudson's intermediate scrutiny test, the Court
7 must examine whether 1) the speech concerns lawful activity and
8 is not misleading; 2) the asserted government interest is
9 substantial; 3) the regulation directly serves that interest; and
10 4) the regulation is no more extensive than necessary to serve
11 that interest. Central Hudson, 447 U.S. at 566. Elaborating on
12 the last factor, the Supreme Court has made clear that "[t]he
13 Government is not required to employ the least restrictive means
14 conceivable, but it must demonstrate narrow tailoring of the
15 challenged regulation to the asserted interest - 'a fit that is
16 not necessarily perfect, but reasonable; that represents not
17 necessarily the single best disposition but one whose scope is in
18 proportion to the interest served.'" Greater New Orleans Broad.
19 Ass'n v. United States, 527 U.S. 173, 188 (1999) (quoting Board
20 of Trustees of State Univ. of N. Y. v. Fox, 492 U.S. 469, 480
21 (1989)); Lorillard Tobacco Co. v. Reilly, 533 U.S. 525, 556
22 (2001) (explicitly stating that case law does not require "the
23 least restrictive means," but only a "reasonable fit."); see also
24 Trans Union v. FTC, 245 F.3d 809, 818-19 (D.C. Cir. 2001)
25 ("Because the FCRA is not subject to strict First Amendment
26 scrutiny . . . Congress had no obligation to choose the least
27 restrictive means of accomplishing its goal."). Furthermore,
28 while the commercial speech test requires more than "mere

1 speculation or conjecture" that the restriction advances the
2 government interest, Greater New Orleans, supra, at 188, neither
3 does it require "a surfeit of background information." Lorillard
4 Tobacco, 533 U.S. at 555. The means used to achieve a
5 permissible goal can be justified "solely on history, consensus,
6 and 'simple common sense.'" Id. (quoting Florida Bar v. Went For
7 It, Inc., 515 U.S. 618, 628 (1995)).

8 The facts of this case meet the first prong of the Central
9 Hudson test, in that copying expiration dates is not misleading
10 and concerns otherwise lawful transactions. Regarding the second
11 prong, Defendant does not, and can not, deny the government's
12 significant interest in preventing identity theft. See Def.
13 Answer at ¶ 42 ("Congressional concern about identity theft was
14 valid."); Trans Union, 245 F.3d at 818 (governmental interest in
15 "protecting the privacy of consumer credit information . . . is
16 substantial."). The dispute, therefore, centers on the third and
17 fourth prongs of Central Hudson, and specifically Defendant's
18 assertion that the combination of an expiration date and a
19 truncated card number cannot possibly be used to facilitate the
20 type of fraud Congress wanted to prevent.

21 Congress sought with FACTA to "assist[] consumers in
22 preventing identity theft and for mitigating its consequences
23 once the crime has occurred." See 108 H. Rep. No. 263 (2003).
24 The goal of the provision that became § 1681c(g) was to "limit
25 the opportunities for identity thieves to 'pick off' key card
26 account information." S. Rep. No. 108-166 (2003). FACTA
27 followed enactment of laws in at least 20 states with provisions
28 similar to § 1681c(g) that prohibited printing the full card

number as well as the expiration date on receipts.² A handful of other states passed laws focused only on the card number.³ As shown by the final language of § 1681c(g), Congress mandated the more comprehensive version of these restrictions as the national standard. Congress' decision to protect both card numbers and expiration dates from inadvertent disclosure through discarded sales receipts, as many states had already done, directly serves the interest Congress sought to protect through the least restrictive means available.

Defendant claims that expiration dates accompanied only by truncated card numbers need no protection from would-be fraudsters. Defendant submitted with its opposition to Plaintiff's motion the declaration of a former MasterCard employee who stated that a full expiration date and a truncated card number cannot be used to make fraudulent transactions. Decl. of Joel Lisker, Dkt. #22. Defendant also contends, based

² See Ariz. Rev. Stat. Ann. § 44-1367 (2001); Ark. Code Ann. § 4-107-303 (West 2003); Cal. Civ. Code § 1747.09 (West 2007); Colo. Rev. Stat. Ann. § 6-1-711 (West 2006); Conn. Gen. Stat. Ann. § 42-133hh (West 2003); Fla. Stat. Ann. § 501.0188 (West 2003); Ga. Code Ann. § 10-15-3 (2007); Idaho Code Ann. § 28-51-103 (2003); 815 Ill. Comp. Stat. Ann. 505/2mm (West 2004); Kan. Stat. Ann. § 50-669b (2002); La. Rev. Stat. Ann. § 9:3518.3 (2001); Me. Rev. Stat. Ann. Tit. 10, § 1149 (2004); Nev. Rev. Stat. Ann. § 597.945 (West 2003); N.J. Stat. Ann. § 56:11-42 (West 2002); N.Y. Gen. Bus. Law § 520-a (McKinney 2003); N.D. Cent. Code § 51-07-27; Ohio Rev. Code Ann. § 1348.18 (West 2002); Okla. Stat. Ann. Tit. 15, § 752a (West 2002); Tex. Bus. & Com. Code Ann. § 35.61 (Vernon 2003); Utah Code Ann. § 13-38-101 (West 2003); Va. Code Ann. § 11-33.2 (West 2004); Wash. Rev. Code Ann. § 19.200.010 (West 2000).

³ See Del. Code Ann. Tit. 11, § 915a (2003); Md. Code Ann., Commercial Law § 14-1318 (West 2003); Mo. Ann. Stat. § 407-433 (West 2003); Neb. Rev. Stat. § 28-633 (2002); N.m. Stat. Ann. § 56-4-3.1 (West 2003); N.c. Gen. Stat. Ann. § 14-113.24 (West 2003); Or. Rev. Stat. Ann. § 646.888 (West 2007); Wis. Stat. Ann. § 134.74 (West 2002).

1 on the same declaration, that card companies routinely complete
2 transactions with incorrect expiration dates so long as the
3 expiration date provided to the merchant is in the future.
4 Def.'s Br. at 3. Therefore, Defendant claims, a restriction on
5 copying expiration dates to sales slips does not advance the
6 government's interest in preventing identity theft and other
7 fraud.

8 Defendant's argument that a thief would not be able to make
9 fraudulent charges using only a truncated card number and the
10 full expiration date misses the point. Thieves might piece
11 together (or "pick off," in the words of Congress) different bits
12 of information from different sources. The expiration date of a
13 customer's credit/debit card, until recently printed on
14 Defendant's receipts, is one of several pieces of information
15 that can make it easier for criminals to rack up fraudulent
16 charges. These dates are worth protecting even when not
17 accompanied by other important financial information.⁴

18 Congress' actions comport with common experience, testimony
19 provided in support of the legislation, and the instructions
20

21 ⁴ Mr. Lisker also opines that an identity thief who
22 obtained information such as a victim's Social Security number
23 could open accounts under the victim's name and make fraudulent
24 charges to those new accounts. Expiration dates of existing,
25 legitimate cards may not be pertinent to someone creating new,
26 fraudulent accounts from scratch. However, the constitutionality
27 of § 1681c(g) does not require that the provision help fight all
28 types of fraud.

25 Mr. Lisker further argues that consumers suffer little or no
26 damage from unauthorized use of their credit cards because of
27 laws and policies limiting their liability. Even if victims
28 themselves rarely incur any direct monetary loss due to credit
card fraud, such losses are paid by consumers everywhere in the
form of higher bank fees or in the costs for goods and services.
Consumer victims also spend valuable time reporting and otherwise
dealing with this type of fraud.

1 credit card companies give to merchants. For instance, Mari J.
2 Frank, author of a declaration cited in Mr. Lisker's declaration,
3 testified to Congress that expiration dates should be eliminated
4 from sales receipts. On May 15, 2003, Ms. Frank advocated for a
5 rule stating that "[n]o company or entity shall print more than
6 the last 5 digits of a credit card number or account number or
7 the expiration date upon any receipt provided to a cardholder."
8 See Testimony of Mari J. Frank, May 15, 2003, before the House
9 Gov't. Reform Comm. (available at 2003 WL 21130287) (emphasis
10 added). Ms. Frank was not alone in pressing Congress to protect
11 expiration dates. Michael D. Cunningham, Senior Vice President
12 of Credit and Fraud Operations for Chase Cardmember Services,
13 testified before the Senate Banking Committee in 2003 that much
14 of the fraud his company encountered occurred when a card
15 "account number and expiration date is compromised[,] permitting
16 purchases by phone, mail, or Internet." See S. Hrg. 108-579,
17 June 19, 2003, before the Senate Comm. on Banking, Housing, and
18 Urban Affairs. Linda Foley, Executive Director of the Identity
19 Theft Resource Center, recommended that Congress require
20 businesses to print only truncated card numbers and no expiration
21 dates on receipts. Id.

22 Anyone who has used a credit or debit card for telephone or
23 online transactions knows that retailers, especially those
24 accepting orders over the phone or through the Internet, require
25 expiration dates to complete transactions. That common
26 experience is borne out by the policies of credit card companies.
27 For example, VISA publishes a handout for merchants entitled "If
28

1 the Card is NOT There - You Need to be MORE Aware." That
 2 document instructs merchants to:

3 Ask the customer for the card expiration date and
 4 include it in your authorization request. An invalid
 5 or missing expiration date can be an indicator that the
 person on the other end does not have the actual card
 in hand.

6 Ex. A.⁵ In another publication called "Rules for VISA
 7 Merchants," VISA again states, in a section entitled "Fraud
 8 Prevention Guidelines for Card-Not-Present Transactions," that
 9 businesses should:

10 Whenever possible, . . . ask customers for their card
 11 expiration, or "Good Thru," date and include it in
 12 [the] authorization requests. Including the date helps
 13 to verify that the card and transaction are legitimate.
 A [mail order/telephone order] or Internet order
 containing an invalid or missing expiration date may
 indicate counterfeit or unauthorized use.

14 Ex. B (excerpts from VISA Rules) at 32 (emphasis added).⁶ Those
 15 same Rules further state:

16 Key-entered transactions are fully acceptable, but they
 17 are associated with higher fraud and chargebacks rates.
 18 In addition, when transactions are key-entered, the
 19 benefits associated with special security features -
such as the expiration date and Card Verification Value
2 (CVV2) - are not available.

20 Rules, p. 31 (emphasis added).⁷

21 ⁵ Available at
 22 http://usa.visa.com/download/merchants/card_not_there_aware.pdf.

23 ⁶ Available at
 24 [http://usa.visa.com/download/merchants/rules_for_visa_merchants.p](http://usa.visa.com/download/merchants/rules_for_visa_merchants.pdf)
 df.

25 ⁷ In her declaration, Ms. Frank quotes another section of
 26 the "Rules for Merchants" document for the proposition that all
 27 expiration dates are automatically considered correct in
 28 telephone, mail, or Internet transactions. See Frank Decl. (Dkt.
 #22, Ex. B) at 5. However, the page from which Ms. Frank quotes
 deals with chargeback "Code 73: Expired Card" and specifies that
 "[m]any Merchant Banks automatically handle this type of
 chargeback, so you never really see it." *Id.* at 103. A

1 Other credit card companies similarly advise merchants to
 2 verify expiration dates as a way of helping to prevent fraud.
 3 Ms. Frank's declaration quotes a "financial crimes expert" with
 4 American Express as stating that "60% of the time the expiration
 5 date is not evaluated for verification purposes." Frank Decl.
 6 (Dkt. #22, Ex. B) at 14. In other words, according to the
 7 documents submitted by Defendant, the expiration date is
 8 evaluated for verification purposes in almost half of American
 9 Express transactions. The "Fraud Prevention Handbook," provided
 10 to merchants by American Express, verifies that merchants should
 11 obtain the expiration date, especially for "card-not-present"
 12 transactions:

13 When you are accepting an American Express Card for
 14 mail, telephone or Internet transactions, obtain the
 Cardmember's:

- 15 1. Name exactly as it appears on the Card
- 16 2. Card account number
- 17 3. Expiration date on the Card (valid date) . . .

18 Call American Express Authorizations . . . to verify
 19 the billing address and CID. Address verification must
 be done for charges when merchandise will be shipped.
 Provide:

- 20 - Cardmember account number
- 21 - Expiration date

22
 23
 24 _____
 25 chargeback occurs when a transaction is reversed and cancelled.
 This section of the "Rules" does not support the broad conclusion
 Ms. Frank draws from it.

26 Furthermore, as stated elsewhere in its Rules for Merchants,
 27 VISA does consider expiration dates to be one way to help verify
 legitimate transactions. The statements of VISA's Joseph Majka,
 28 as related in Ms. Frank's declaration, do not address the issue
 of whether expiration dates are sometimes used to help verify
 transactions as legitimate. See Frank Decl. at 8.

1 Ex. C (Excerpts from American Express "Handbook") at 38.⁸
2 American Express also urges merchants not to print expiration
3 dates on receipts in order to protect that information against
4 fraud:

5 As an American Express merchant, you are responsible
6 for helping to ensure that your customer's credit card
7 information is secured and protected against future
8 fraud activity. Here are a few steps that you can take
9 to protect this information:

10 . . . Do not print the Card expiration date or your merchant
11 account number on the terminal (customer) receipt. Only
12 print a "subset" of the Card account numbers on the terminal
13 (customer) receipt.

14 Id. at 39 (emphasis added).

15 The company that manages the Discover Card also requests
16 that merchants obtain expiration dates when processing online or
17 over-the-phone orders. See Ex. D at 41.⁹ In an online document
18 entitled "Fraud Prevention/Card Not Present," Discover explains
19 to merchants that the "Types of Suspicious Behavior" potentially
20 indicative of fraud includes when a "[c]ustomer instructs you to
21 try different expiration dates when initial attempts fail." Ex.
22 E (emphasis added) at 44.¹⁰

23 As illustrated by these instructions from credit card
24 companies to merchants, expiration dates should be used to
25 evaluate the legitimacy of transactions. If a customer provides

26 ⁸ Available at
27 [https://www209.americanexpress.com/merchant/singlevoice/resources](https://www209.americanexpress.com/merchant/singlevoice/resources/FPHANDcvr.pdf)
28 [/FPHANDcvr.pdf](https://www209.americanexpress.com/merchant/singlevoice/resources/FPHANDcvr.pdf).

⁹ Available at
http://www.discovernetwork.com/home/data/fraud_faq.html.

¹⁰ Available at
[http://www.discovernetwork.com/resources/data/card_not_present.ht](http://www.discovernetwork.com/resources/data/card_not_present.html)
[ml](http://www.discovernetwork.com/resources/data/card_not_present.html).

1 an expiration date that does not match the true date, the
2 authorization may fail. Expiration dates may not be examined in
3 every case; the thoroughness of the verification process is
4 determined to a large extent by individual merchants, their
5 banks, and the customer's card issuer. But expiration dates
6 plainly are not extraneous information, as Defendant suggests.
7 Checking expiration dates and protecting them from casual
8 disclosure is one method that credit card companies, banks, and
9 merchants employ to prevent fraud. See Decl. of Don Coker
10 (submitted with Pl.'s Reply to Def.'s Opp'n. to Pl.'s Mot. to
11 Dismiss Counterclaim) at ¶ 14 (purchase declined at online
12 retailer due to invalid expiration date). Even if that does not
13 happen in every single case, intermediate scrutiny does not
14 obligate courts to invalidate a "remedial scheme because some
15 alternative solution is marginally less intrusive on a speaker's
16 First Amendment interests." Turner Broad. System, Inc. v. FCC,
17 520 U.S. 180, 217-18 (1997) (citations omitted). "So long as the
18 means chosen are not substantially broader than necessary to
19 achieve the government's interest, . . . [a] regulation [is] not
20 . . . invalid simply because a court concludes that the
21 government's interest could be adequately served by some
22 less-speech-restrictive alternative." Id. at 218 (quotation
23 omitted).

24 Here, Congress reasonably determined that expiration dates
25 should be protected, and that conclusion led directly to the
26 extremely limited restriction on the "speech" embodied by
27 § 1681c(g). "[T]he government cannot promote its interest
28 (protection of personal financial data) except by regulating

1 speech because the speech itself (dissemination of financial
2 data) causes the very harm the government seeks to prevent."
3 Trans Union v. FTC, 267 F.3d 1138, 1141 (D.C. Cir. 2001). The
4 restriction, in other words, directly serves the government's
5 interest by means no more restrictive than necessary. In fact,
6 the prohibition affects no other speech whatsoever, either
7 indirectly or unintentionally. It does not even prevent
8 Defendant from doing what it claims to do by printing such
9 information: Customers can confirm that transactions were
10 properly charged by looking at the truncated card number and
11 other information on the receipt, without the expiration date.
12 In any calculation of the costs and benefits of § 1681c(g), the
13 "cost" column would have to be set at zero. It easily passes the
14 Central Hudson test.

15 CONCLUSION

16 Section 1681c(g) directly advances the government's
17 legitimate interest in preventing identity theft and related
18 fraud by means that are as narrowly tailored as possible.
19 Furthermore, the terms of the statute are clear. The United

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //

28 //

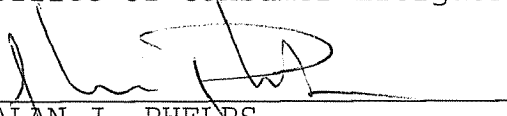
1 States asks that this Court find the provision constitutional, if
2 it determines that it must reach the constitutional question at
3 all.

5 Respectfully submitted,

6 PETER D. KEISLER
7 Assistant Attorney General
8 Civil Division
9 United States Department of Justice

10 EUGENE M. THIROLF
11 Director
12 Office of Consumer Litigation

13 Dated: July 24, 2007


14 ALAN J. PHELPS
15 Office of Consumer Litigation
16 U.S. Department of Justice
17 1331 Penn. Ave. NW Suite 950N
18 Washington, DC 20004

19 Attorneys for the United States
20
21
22
23
24
25
26
27
28

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Brief of the United States in Support of 15 U.S.C. § 1681c(g) was sent via electronic mail and facsimile this 24th day of July, 2007, to the following:

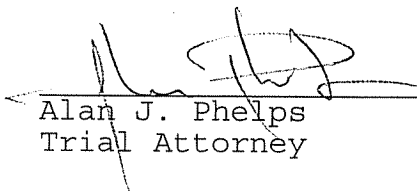
Camille E. Bennett
Harold C. Hirshman
Sonnenschein Nath & Rosenthal
7800 Sears Tower
Chicago, IL 60606
fax: (312) 876-7934

David H. Stern
Sonnenschein Nath & Rosenthal
601 S. Figueroa St., Ste. 1500
Los Angeles, CA 90017-5704
fax: (213) 623-9924

Attorneys for Defendants

Launa Nicole Everman
Wayne S. Kreger
Milstein Adelman and Kreger
2800 Donald Douglas Loop North
Santa Monica, CA 90405
fax: (310) 396-9635

Attorneys for Plaintiff



Alan J. Phelps
Trial Attorney

Exhibit A



With the proper know-how and the right tools, mail order, telephone and Internet merchants can detect fraud and avoid associated card losses.

If the Card is NOT There — You Need to be MORE Aware

To stay ahead of the crooks and reduce your fraud exposure:

- 1 Ask the customer** for the card expiration date and include it in your authorization request. An invalid or missing expiration date can be an indicator that the person on the other end does not have the actual card in hand.
- 2 Use fraud detection** tools like the Address Verification Service (AVS) and Card Verification Value 2 (CVV2) as part of the authorization process. To order the Merchant Guide to AVS (VRM 01.01.06) or the Merchant Guide to CVV2 (VRM 03.14.06) call 1-800-VISA-311 or visit www.visa.com/merchant.
- 3 Be on the lookout** for questionable transaction data or other signs indicating “out of pattern” orders.

If you suspect fraud:

- **Ask the customer** for day/evening phone numbers, then call the customer with any questions.
- **Ask for additional information** (e.g., bank name on the front of card).
- **Separately confirm the order** by sending a note via the customer’s billing address, rather than the “ship to” address.

Report suspicious activity to your merchant bank.



Exhibit B



Rules for Visa Merchants

Card Acceptance and Chargeback Management Guidelines





VisaNet® is part of Visa's consumer payment system. It is itself a collection of systems that includes:

- **An authorization service** through which issuers can approve or decline individual Visa card transactions.
- **A clearing and settlement service** that processes transactions electronically between merchant banks and issuers to ensure that:
 - Visa transaction information moves from merchant banks to issuers for posting to cardholders' accounts.
 - Payment for Visa transactions moves from issuers to merchant banks to be credited to the merchant's account.

Transaction Life Cycles

The following illustrations show the life cycle for Visa card transactions, for both card-present and card-not-present purchases. Processing events and activities may vary slightly for any one merchant, merchant bank, or card issuer, depending on card and transaction type, and the processing system used.

Authorization

1. Cardholder presents a Visa card to pay for purchases. For card-not-present transactions, the cardholder provides the merchant with the account number, expiration date, billing address, and CVV2.

2. Merchant swipes the card, enters the dollar amount, and transmits an authorization request to the merchant bank. For card-not-present transactions, the account number and other information may be digitally or key-entered.

3. Merchant bank electronically sends the authorization request to VisaNet.

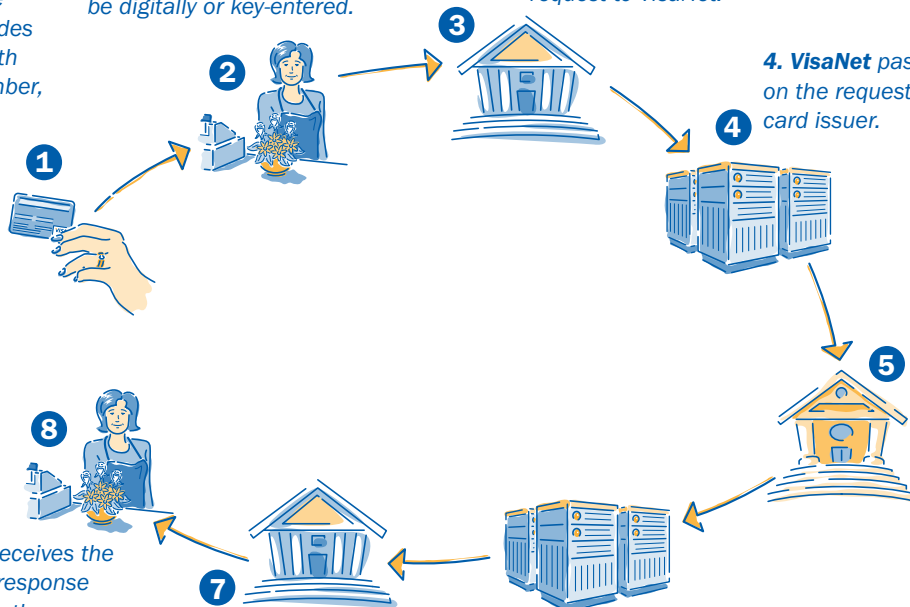
4. VisaNet passes on the request to the card issuer.

5. Card issuer approves or declines the transaction.

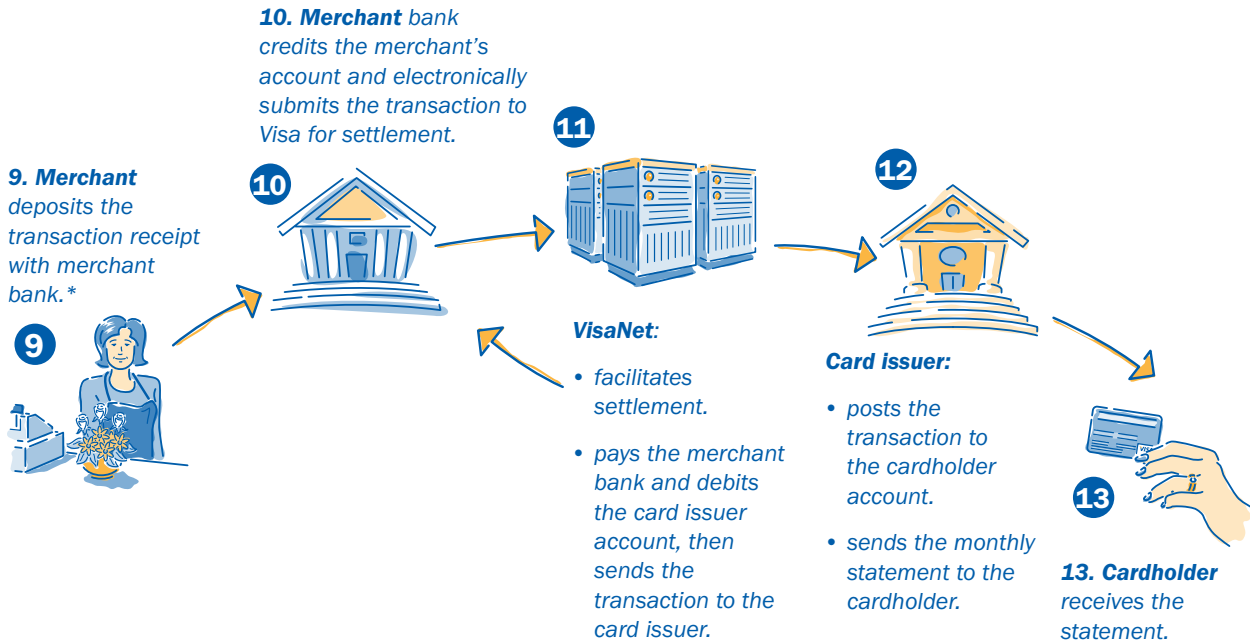
6. VisaNet forwards the card issuer's authorization response to the merchant bank.

7. Merchant bank forwards the response to the merchant.

8. Merchant receives the authorization response and completes the transaction accordingly.



Clearing and Settlement



*Merchants or their agents that store, process, or transmit data may not store sensitive authentication data (full magnetic-stripe or chip) contents. Card Verification Value 2 (CVV2), or PIN Verification Value (PVV)—even if it is encrypted. Once an authorization is processed, such data should no longer exist. The only components of the magnetic stripe that can be stored are name, account number, and expiration date.

DCC Transaction Receipt Requirements

For both a card-present or card-not-present environment, a DCC transaction must contain all of the following:

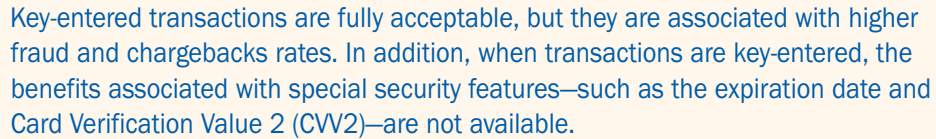
- Transaction amount of the goods or services purchased in the merchant's local currency—including currency symbol next to the amount
- Exchange rate, including any commission
- Total price in the transaction currency, accompanied by the words "Transaction Currency"—including currency symbol next to the amount
- A disclaimer that:
 - is easily visible to the cardholder,
 - specifies that the cardholder has been offered a choice of payment in the merchant's local currency, and that the cardholder understands the choice of currency is final

Fashion Store Location Date and Time	
Merchant ID	xxxxx
Terminal ID	xxxxx
Date:	Time:
Invoice No:	Auth No:
VISA	SALE
Card No	xxxxxxxxxxxx6330
Exp. Date	xx/xx
Sale Amount	100 Merchant Currency
Tax	2
Total Amount	102 Merchant Currency
Exchange Rate:	
+ Commission: xx.xx	
Sale Amount	\$ 65 Transaction Currency
I accept that I have been offered a choice of currencies for payment & that this choice is final.	
Signature: _____	

Truncated Account Number

Visa requires that all new electronic POS terminals provide account number truncation on transaction receipts. This means that only the last four digits of an account number should be printed on the customer's copy of the receipt.

After July 1, 2006, the expiration date should not appear at all. Existing POS terminals must comply with these requirements by July 1, 2006. To ensure your POS terminals are properly set up for account number truncation, contact your merchant bank.



These best practices can help you keep key-entered transactions at acceptably low levels and should be incorporated into your daily operations and staff training and review sessions.

Calculate the percentage of key-entered transactions compared to total transactions to pinpoint which stores, terminals, or sales associates have high key-entry rates. Merchants are encouraged to monitor their key-entry rates on a monthly basis.

To obtain the percentage of key-entered transactions for a particular terminal, divide the total number of key-entered transactions by the total number of sales. Exclude from both totals any mail or telephone orders that may have been made at the terminal. Perform the above calculation for each terminal, and for each sales shift to determine the key-entry rate per sales associate. Repeat the process for each store, as appropriate.

If your key-entry rates are greater than one percent per terminal or sales associate, you should investigate the situation and try to find out why. The following chart summarizes the most common reasons for high key-entry rates and provides possible solutions.

22

Fraud Prevention Guidelines for Card-Not-Present Transactions

Visa has established a range of fraud-prevention policies, guidelines, and services for card-not-present merchants. Using these tools will help protect your business from fraud-related chargebacks and losses. MO/TO and Internet merchants should strongly consider developing in-house fraud control policies and providing appropriate training for their employees.

The following sections outline basic fraud-prevention guidelines and best practices for card-not-present merchants.

Authorize All Card-Not-Present Transactions

Authorization is required on **all** card-not-present transactions. Card-not-present transactions are considered as zero-floor-limit sales. Authorization should occur before any merchandise is shipped or service performed.

Ask for Card Expiration Date

Whenever possible, card-not-present merchants should ask customers for their card expiration, or “Good Thru,” date and include it in their authorization requests.

Including the date helps to verify that the card and transaction are legitimate. A MO/TO or Internet order containing an invalid or missing expiration date may indicate counterfeit or other unauthorized use.

Ask for CVV2

The Card Verification Value 2 (CVV2) is a three-digit security number printed on the back of Visa cards to help validate that a customer is in possession of a legitimate card at the time of an order. (See *Visa Card Features and Security Elements* on page 23.)

Studies show that merchants who include CVV2 validation in their authorization procedures for card-not-present transactions can reduce their fraud-related chargebacks.

CVV2 Processing

To ensure proper CVV2 processing for card-not-present transactions, merchants should:

- ✓ Ask card-not-present customers for the last three numbers in or beside the signature panel on the back of their Visa cards.

Section 7:

Chargeback Reason Codes

The chargebacks discussed in this section are grouped into six classifications:

- ✓ Non-Receipt of Information
- ✓ Fraud Codes
- ✓ Authorization Errors
- ✓ Processing Errors
- ✓ Cancelled or Returned
- ✓ Non-Receipt of Goods or Services

Reason Code 73: Expired Card

Definition	The card issuer received a transaction that was completed with an expired card and was not authorized.
Most Common Causes	The merchant accepted a card after its expiration or "Good Thru" date and did not obtain an authorization approval from the card issuer.
Merchant Actions	Back-Office Staff Card Not Expired—Key-Entered Transaction (PR) For key-entered transactions, the expiration date should be on the manually imprinted copy of the front of the card. If the expiration date on sales receipt shows the card had not expired at the time of the sale, send a copy of the receipt to your merchant bank. The chargeback is invalid regardless of whether authorization was obtained. Card Expired, Authorization Obtained (PR) If the card was swiped or a manual imprint made, an authorization approval was obtained as required, inform your bank of the transaction date and amount. Many merchant banks automatically handle this type of chargeback so you never see it. Card Expired, No Authorization Obtained (NR) If the card is expired and you did not obtain an authorization, accept the chargeback. Point-of-Sale Staff Check Expiration Date (PM) Check the expiration or "Good Thru" date on all cards. A card is valid through the last day of the month shown; for example, if the Good Thru date is 04/08, the card is valid through April 30, 2008 and expires on May 1, 2008. Card-Not-Present, Authorization Obtained (PR) If the transaction was a MO/TO or Internet transaction, then the expiration date provided by the cardholder is considered correct. Many merchant banks automatically handle this type of chargeback, so you really never see it.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Reason Code 73: Expired Card (continued)

Always Get Authorization Approval for Expired Cards

(PM) Always request an authorization for transactions on expired cards and submit the expiration date on the card as part of the authorization request. The expiration date is submitted automatically when you swipe a card. If a transaction is not approved, do not complete the sale.

Owner/Manager

Check Card Expiration Date

(PM) Periodically remind point-of-sale staff to check the card's expiration date before completing transactions and to always obtain an authorization approval if the card is expired.

Merchant Actions Legend:

(PR) Possible Remedy (PM) Preventive Measure (NR) No Remedy (CS) Customer Service Suggestion

Exhibit C



American Express

Fraud Prevention Handbook

Mail Order, Telephone Order, Internet Order Acceptance Procedures

Since mail, telephone and Internet orders are more susceptible to Card fraud, American Express has designed procedures to help protect the Cardmember and the Service Establishment. By following these procedures, you may prevent a criminal from obtaining merchandise or services at your expense.

When you are accepting an American Express Card for mail, telephone or Internet transactions, obtain the Cardmember's:

1. Name exactly as it appears on the Card
2. Card account number
3. Expiration date on the Card (valid date)
4. Card Identification (CID) number (if your establishment is certified to verify the Card Identification Number)

The CID is a 4-digit number printed above the account number on the face of all American Express Cards. The Card Identification number can help you control fraud:

- The Customer must have the actual Card; carbons and old receipts do not display this number.
 - The CID has the advantages of a personal identification number without the problems. Cardmembers don't have to remember a special code; it's printed on the Card.
 - Fraud associated with stolen Card numbers is greatly reduced as the CID changes each time a new card is issued.
5. Billing address, and the address where the merchandise is to be shipped, (if different from the billing address)

Automatic Address Verification (AAV)

In our on-going commitment to help eliminate fraud in the phone and mail order industry, American Express offers Automatic Address Verification (AAV) for American Express transactions. This system electronically transmits your customer's address and zip code to our Cardmember's file. You receive a code indicating a complete, partial, or no-match for each transaction to help you make informed shipping decisions. AAV is free to merchants and qualified third-party processors. For additional information regarding AAV, contact your American Express Account Representative.

6. Billing address phone number and home or business number
7. Phone number where the Cardmember can be reached (if different from the home or business phone)



Mail Order, Telephone Order, Internet Order Acceptance Procedures (continued)

Additionally:

- If you submit electronically, your electronic Charge Record should indicate "Mail Order," "Phone Order" or "Internet" on the Cardmember billing statement.
- Select shippers that do not allow shipment re-routes.
- If phone/Internet orders are allowed to be picked up at retail locations, require the Card to be presented.

Authorization Procedures

Call American Express Authorizations at (1-800-528-2121) to verify the billing address and CID. Address verification must be done for charges when merchandise will be shipped. Provide:

- Cardmember account number
- Expiration date
- Name as it appears on the Card
- Cardmember billing address
- Card Identification Number

You will be told "yes" or "no" depending on whether or not the billing address and CID match our files. **Remember that the billing address verification and the CID verification are checks, not guarantees that the charge is legitimate.**



The risk of fraud is greater during transactions where the card is not present. Therefore it is important to follow proper security procedures.

Mail Order, Telephone Order, Internet Order Acceptance Procedures (continued)

Reducing Fraud and Chargeback Risk

When the billing address is confirmed but delivery will be to a different address, you help reduce the risk of fraud and chargebacks if you:

- Call back the Cardmember to validate the order. Be sure not to call the phone number received with the order; check the telephone directory, if possible.
- Another way to help control future fraud and chargeback losses is to suppress printing the Card number on the shipping invoice. Instead, you may wish to block out all but the last 4 or 5 digits of the 15-digit Card number (see example – Information Protection, p.9). Additionally, never print the CID number on the shipping invoice.
- Be wary of situations where someone places a telephone order, then sends someone (who does not present the Card) to pick up the merchandise.
- Do not accept a fax of the Card as a valid presentation.
- If transactions are done via the Internet, ensure that sites are secured for electronic commerce with the main emphasis of protecting unauthorized access to the customer card information (e.g., behind a firewall). Transactions should be conducted using browser software that supports industry-standard encryption protocols. Passwords to Merchant Web sites should be changed regularly and never set to default.



As Internet orders become more commonplace, it is important that your procedures include a thorough check of each customer.

Reminders:

- If you fulfill an order more than 30 days after the original authorization, call again for a new approval code before mailing the merchandise.
- Charges cannot be submitted for payment until the merchandise is shipped.

Information Protection/Data Security

As an American Express merchant, you are responsible for helping to ensure that your customer's credit card information is secured and protected against future fraud activity. Here are a few steps that you can take to protect this information:

1. Customer's credit card information should be kept confidential. Any electronically stored Cardmember information should be encrypted and/or password protected. (Consult your Terminal Provider or local software specialty store for assistance.)
2. Store your daily credit card receipts in a secured area and limit access to this information to personnel that need this information for accounting and customer service purposes only.
3. Credit card information that is discarded should be shredded or destroyed. Always destroy unneeded carbon copies of charge forms, lodging portfolios or car rental agreements to prevent misuse of valuable Cardmember information.
4. Do not print the Card expiration date or your merchant account number on the terminal (customer) receipt. Only print a "subset" of the Card account numbers on the terminal (customer) receipt.
5. Only your terminal provider or Helpdesk Representative should make changes or upgrades to your Point of Sale equipment and transmission lines.
6. Monitor behavior and activities of employees, especially in transactions where the Card is out of the customer's possession. Ensure that portable and hand held card reading/capturing devices are not being used by employees to capture card data. Be wary of a "contact person" that shows up regularly to meet with an employee to drop off/pick up a scanner, or to pay off an employee for data that has been collected.

Merchant Name
Street Address
City State Zip Code
Telephone Number

Purchase \$ 53.46

C F FR05T
American E # XXXXXXXXXXXX1008
Auth # 236743
05/25/00 1p:51 Re # 0010013750

Signature: _____
C F FR05

I AGREE TO PAY ABOVE TOTAL AMOUNT
ACCORDING TO CARD ISSUER AGREEMENT

Only print a "subset" of the Card
account number on the receipt.

Exhibit D



[Register to Use Discovernetwork.com](#)

▶ [About Us](#)
[Help & FAQs](#)

[General FAQs](#)
[Reporting FAQs](#)
[Submission Error Fees](#)
[FAQs](#)
[Internet FAQs](#)
[Rules and Regulations](#)
[Fraud Prevention](#)
[Fraud Prevention FAQs](#)
[System Requirements](#)
[Account Activation](#)
[Gift Card FAQs](#)
[Online Advertising FAQs](#)
[Automatic Payments](#)
[FAQs](#)

[Privacy](#)

▶ [Contact Us](#)
[Site Map](#)
[Terms of Use](#)
[Discover Network](#)
[Acceptance Mark -](#)
[Guidelines and Logos](#)

Help Topics

Fraud Prevention - Ask The Expert (FAQs)

1. [How can I prevent fraud?](#)
2. [How can I prevent Internet, Mail-Order \(MO\) and Telephone-Order \(TO\) fraud?](#)
3. [Why should I require CID on my Web site?](#)
4. [Why should I require a signature when delivering mail or telephone orders?](#)
5. [Why is data security so important and how can I protect my business and customers from hacking attacks?](#)
6. [Where can I report suspected Merchant Fraud?](#)
7. [Where can I meet other Merchants that may have the same Card Not Present \(CNP\) fraud concerns that I have?](#)
8. [What are some signs of suspicious behavior?](#)
9. [What do I do if I suspect a Card is fraudulent in a Card Present situation?](#)
10. [What are some tools offered by Discover Network to help prevent fraud?](#)

1. How can I prevent fraud?

There isn't a single simple solution or tool to preventing fraud. It takes an assortment of many tools to prevent fraud. The best protection comes from knowledge and understanding of the latest tools and trends impacting the marketplace. Discover Network offers its Merchants numerous tools to assist in the fight against fraud. Reading through the FAQs listed below will help you determine what your business needs to do to reduce your fraud risk. Awareness is the first step towards fighting fraud!

2. How can I prevent Internet, Mail-Order (MO) and Telephone-Order (TO) fraud?

Here are some guidelines for preventing Internet and MO/TO fraud:

Request Cardholders for the following information during the order taking process:

- Cardmember Name, exactly how their name appears on their Discover® Network-issued card
- Card Account Number is at least 16 digits
- Card Expiration Date, four-digit number MM/YY
- [CID \(Card Identification Data\)](#), the three-digit number located on the back of the card in the signature panel
- Card billing address along with the ship-to address (when necessary)
- Home, business or other telephone number where the Cardmember can be reached

For each transaction, be sure to:

- Request and validate the [Card Identification Data \(CID\)](#) (the three-digit code on the back of the card in the signature panel). The CID can be submitted in the electronic authorization request or can be used when calling our authorization center
- Verify the customer's billing address, either electronically or by our automated

Exhibit E



- ▶ [Merchant Resources](#)
- ▶ [Home](#)
- ▶ [Order Signage & Supplies](#)
- ▶ [Fraud Prevention](#)
- ▶ [Card Present](#)
- ▶ [Card Not Present](#)
- ▶ [Discover Network](#)
- ▶ [Security Features](#)
- ▶ [Internet and Protecting](#)
- ▶ [Customer Information](#)
- ▶ [Internet Fraud Alert](#)
- ▶ [Abbreviated Numbers](#)
- ▶ [Fraud Prevention Supplies](#)
- ▶ [Ask the Expert \(FAQs\)](#)
- ▶ [Data Security](#)
- ▶ [Discover Network Gift](#)
- ▶ [Card Products](#)
- ▶ [Payroll Cards](#)
- ▶ [Contactless Payments](#)
- ▶ [Biometrics](#)
- ▶ [Merchant Offers](#)
- ▶ [Online Advertising](#)
- ▶ [Automatic Payments](#)
- ▶ [Change Your Bank](#)
- ▶ [Account Information](#)
- ▶ [Rules and Regulations](#)
- ▶ [Activate Your](#)
- ▶ [Terminal / POS Device](#)
- ▶ [Transaction Processors](#)

Fraud Prevention

Card Not Present

In any situation where a card is not present and you are unable to complete a face-to-face transaction, the opportunity for fraud increases.

Card Not Present (CNP) transactions have become the foundation for commerce over the Internet in addition to mail order and telephone order businesses. To assist your company in reducing fraud exposure, these helpful tips have been developed for Discover® Network Merchants who are doing business in a CNP environment.

- [Authorization Center](#)
- [Helpful Hints to Reduce Chargebacks and Risks](#)
- [Types of Suspicious Behavior](#)

Authorization Center

To obtain an authorization or address verification, or to question the validity of a Discover® Network Issued Credit Card, please call **1-800-347-1111**.

Helpful Hints to Reduce Chargebacks and Risks

- Request and validate the [Card Identification Data](#) (CID) (the three-digit code on the back of the card in the signature panel). The CID can be submitted in the electronic authorization request or can be used when calling our authorization center
- Verify the customer's billing address, either electronically or by our automated phone system (Address Verification System - AVS)
- Check your delivery service contract for who is responsible for merchandise not delivered
- Get a signature for each delivery
- Keep all delivery records
- All declines are final. Do not force through any sales for which you have received any declined response to your authorization request
- If the sale is on a credit card, do not refund in cash or by check. Refund sales on the same card account that the purchase was made on
- Include your common DBA and customer service number on the Cardholder's transaction statement
- Clearly communicate any and all delivery charges, restocking or other fees
- Clearly explain any return policies and offer documentation of this policy with each sale
- When working on a chargeback, document efforts to satisfy the customer
- Respond to all Chargebacks, even the small ones (remember, this is your customer)
- Duplicate charges, or installment plans, unless otherwise stated, require an authorization for each sale

Types of Suspicious Behavior

Please consider that these are only indicators of higher risk transactions. One behavior

alone may not be a concern.

- New customer attempts to make a very large credit card transaction
- Customer doesn't know the [Card Identification Data](#) (CID) found on the back of the Card, indicating that they don't have the actual Card
- Customer's address does not match when attaining an Address Verification
- Shipping to an address other than the billing address
- Customer asks that you try lower dollar amounts when a decline message is received
- Customer instructs you to try different expiration dates when initial attempts fail
- Customer hesitates, or has a long pause, when asked for personal information
- Customer repeatedly sends e-mail messages requesting confirmation of shipment
- Customer attempts to place multiple orders to the same address
- Customer attempts to purchase large quantities of a single item
- Customer purchases several large-ticket items, which do not go together, e.g., appear random
- Customer calls a few minutes before closing and wants several large-ticket items
- Customer requests that sales be split up to avoid paying "import taxes" and/or "duty fees"
- Customer requests shipment to an overseas destination
- Customer seems overly concerned about delivery time frames to overseas destinations
- Customer attempts to place a large order using several credit cards to obtain the total authorization amount
- Customer offers the phone number to an authorization center to speed up the credit card approval process
- Customer has little regard for price
- Customer shows little or no concern for return policies, manufacturer warranties and/or rebates when purchasing in large quantities

*Please refer to your Discover Network [Merchant Operating Regulations](#) for further Card Not Present (CNP) requirements with respect to the submission of sales.

If there is a breach in your system, notify Discover® Network Security within 48 hours at 1-800-347-3083.

Click [here](#) to learn more about our Data Security guidelines and our DISC program.

For more extensive information on fraud prevention, including identifying the Discover Card brand, handling suspicious situations, and recovering lost or stolen cards, please consult your Discover Network [Merchant Operating Regulations](#).

In our efforts to assist our Merchants that conduct e-commerce transactions, Discover Network is a proud sponsor of the Merchant Risk Council. [Learn more](#).

[Fraud Prevention Supplies](#)

[Back to Top](#) 

[Register](#) [About Us](#) [Terms of Use](#) [Privacy](#) [Help & FAQs](#) [Contact Us](#) [Site Map](#)

© 2007 DFS Services LLC

CIVIL COVER SHEET

The JS44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

BRIAN NOWE, on behalf of himself and all others similarly situated,

DEFENDANT(S)

ESSEX TECHNOLOGY GROUP, LLC (d/b/a Bargain Hunt);
and DOES 1 through 20, inclusive,

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Cobb County

(EXCEPT IN U.S. PLAINTIFF CASES)

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT _____

(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

Charles Austin Gower Jr. (austin@cagower.com)
Shaun Patrick O'Hara (shaun@cagower.com)
CHARLES A. GOWER PC, 1425 Wynnton Road, P.O.
Box 5509, Columbus, GA 31906, Telephone:
706.324.5685; Facsimile: 706.322.2964

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☒ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☐ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

- | PLF | DEF | | PLF | DEF | |
|----------------------------|----------------------------|---|----------------------------|----------------------------|---|
| ☐ 1 | ☐ 1 | CITIZEN OF THIS STATE | ☐ 4 | ☐ 4 | INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE |
| ☐ 2 | ☐ 2 | CITIZEN OF ANOTHER STATE | ☐ 5 | ☐ 5 | INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE |
| ☐ 3 | ☐ 3 | CITIZEN OR SUBJECT OF A FOREIGN COUNTRY | ☐ 6 | ☐ 6 | FOREIGN NATION |

IV. ORIGIN (PLACE AN "X" IN ONE BOX ONLY)

- ☒ 1 ORIGINAL PROCEEDING
- ☐ 2 REMOVED FROM STATE COURT
- ☐ 3 REMANDED FROM APPELLATE COURT
- ☐ 4 REINSTATED OR REOPENED
- ☐ 5 TRANSFERRED FROM ANOTHER DISTRICT (Specify District) _____
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION

(CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

15 U.S.C. §§ 1681 et seq., Fair Credit Reporting Act

(IF COMPLEX, CHECK REASON BELOW)

- | | |
|---|---|
| ☐ 1. Unusually large number of parties. | ☐ 6. Problems locating or preserving evidence |
| ☐ 2. Unusually large number of claims or defenses. | ☐ 7. Pending parallel investigations or actions by government. |
| ☐ 3. Factual issues are exceptionally complex | ☐ 8. Multiple use of experts. |
| ☐ 4. Greater than normal volume of evidence. | ☐ 9. Need for discovery outside United States boundaries. |
| ☒ 5. Extended discovery period is needed. | ☐ 0. Existence of highly technical issues and proof. |

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____	AMOUNT \$ _____	APPLYING IFP _____	MAG. JUDGE (IFP) _____
JUDGE _____	MAG. JUDGE _____ (Referral)	NATURE OF SUIT _____	CAUSE OF ACTION _____

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)CONTRACT - "0" MONTHS DISCOVERY TRACK

- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK

- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK

- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☐ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK

- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☐ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK

- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK

- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK

- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK

- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK

- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK

- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK

- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EML. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK

- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK

- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK

- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK

- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK

- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 490 CABLE/SATELLITE TV
- ☒ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK

- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK

- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND \$ _____

JURY DEMAND ☒ YES ☐ NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE _____ DOCKET NO. _____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)

- ☐ 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- ☐ 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- ☐ 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):

- ☐ 7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. _____, WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.

/s/ Shaun Patrick O'Hara

February 9, 2018

SIGNATURE OF ATTORNEY OF RECORD

DATE

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Georgia Man Claims Bargain Hunt Stores Print Too Many Credit Card Digits on Receipts](#)
