Northwestern Journal of Technology and Intellectual Property

Volume 9 | Issue 8 Article 4

Summer 2011

Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-mail Receipts

Jason Fitterer
Northwestern University School of Law

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-mail Receipts

Jason Fitterer

Summer 2011 VOL. 9, NO. 8

Northwestern Journal of Technology and Intellectual Property
Volume 9, Number 8 (September 2011)

Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-mail Receipts

By Jason Fitterer*

INTRODUCTION

¶1 In a case of first impression at the appellate level, the Seventh Circuit affirmed a district court ruling in *Shlahtichman v. 1-800 Contacts*, confirming that e-mail receipts are outside the scope of federal legislation that requires consumer credit card numbers to be truncated as a measure to fight identity theft and credit card fraud.[1] However, due to the widespread use of e-mail receipts in today's ever-increasing online marketplace and the risks consumers face when their credit card number and expiration date are not truncated on these receipts, this Comment proposes that federal legislation be amended to specifically include e-mail receipts and other electronic communication within its scope.

¶2 In *Shlahtichman*, the plaintiff ordered contact lenses from defendant 1-800 Contacts, which subsequently sent Shlahtichman an automatically generated e-mail confirming his purchase. This e-mail confirmation contained the expiration date of Shlahtichman's credit card. Shlahtichman filed suit, alleging this violated the Fair and Accurate Credit Transactions Act's (FACTA) requirement that credit card numbers be truncated and expiration dates be omitted from "electronically printed" receipts.[2] The district court and appellate court both held that the ordinary meaning of the term "print" does not contemplate the viewing of e-mail on a computer screen, and that the overall language, context, and legislative history of FACTA suggest that the Act was not intended to apply to such receipts.

¶3 Part I of this Comment provides an overview of identity theft and credit card fraud, discussing the prevalence and cost of these crimes, and the common methods by which they are carried out. Part II discusses federal legislation designed to combat identity theft, specifically the Fair Credit Reporting Act (FCRA) and the amendments to FCRA introduced by FACTA. Part III discusses the recent case *Shlahtichman v. 1-800 Contacts*, detailing the reasoning that both the district and appellate courts used to reach their decisions. Part IV proposes that Congress amend FACTA to specifically include e-mail receipts and confirmations within the scope of the Act and provides reasons why amending FACTA is a necessary measure toward further empowering consumers in the fight against identity theft and credit card fraud.

---

* J.D. Candidate 2012, Northwestern University School of Law
[1] Shlahtichman v. 1-800 Contacts, Inc., 615 F.3d 794 (7th Cir. 2010).
[2] 15 U.S.C. § 1681c(g)(1) (2006).

OVERVIEW OF IDENTITY THEFT AND CREDIT CARD FRAUD

¶4 Movie-goers have long been regaled with tales of identity theft in what is perhaps its most blatant and remarkable form: the complete takeover of another's very being, as carried out by such characters as Frank Abagnale, Jr. in *Catch Me If You Can*, Tom Ripley in *The Talented Mr. Ripley*, and, even more recently, on the small screen by the character Don Draper in the AMC television series *Mad Men*.[3] For some, the term identity theft might first bring to mind these elaborate, dramatic plots of popular movies and TV shows in which an impostor takes over another's identity and assumes the victim's life entirely and indefinitely.

¶5 In reality, the overwhelming majority of identity theft occurs on a smaller scale and affects everyday individuals who unwittingly become the victims of fraudulent credit card purchases, loan agreements, and insurance scams. Generally speaking, identity theft encompasses all incidents where someone assumes another's identity in order to perform a fraudulent or criminal act, usually by either accessing that person's existing resources or obtaining new resources with personal information (e.g., loans, credit cards, and other official documents).[4]

A. The Prevalence and Cost of Identity Theft and Credit Card Fraud

¶6 According to a report by the Federal Trade Commission, identity theft was the most frequent consumer complaint to U.S. law enforcement in 2009, comprising 21% of all consumer complaints.[5] In 2009, the number of identity theft and fraud victims rose to over 11 million adult consumers in the U.S. alone.[6] Credit card fraud was the most common form of identity theft reported in 2009, comprising 17% of all identity theft complaints.[7] Specifically, 7% of all identity theft complaints were filed to reporting a fraudulent charge on an existing credit card account.[8] This type of identity theft is most relevant to the discussion in this Comment.

¶7 Most individual victims of identity theft do not experience any personal cost because most banks and credit card issuers have zero-liability policies in place to reimburse any fraudulent charges. However, victims of identity theft in 2009 who did

---

[3] *See generally* CATCH ME IF YOU CAN (DreamWorks SKG 2002); THE TALENTED MR. RIPLEY (Miramax International, Paramount Pictures 1999); *Mad Men* (AMC television broadcast 2007–2010).

[4] *Common Fraud Schemes*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/scams-safety/fraud/fraud#id (last visited Aug. 12, 2011).

[5] FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK FOR JAN.–DEC. 2009, at 3 (2010), *available at* http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf [hereinafter FTC DATA BOOK].

[6] JAVELIN STRATEGY & RESEARCH, 2010 IDENTITY FRAUD SURVEY REPORT: CONSUMER VERSION 5 (2010), *available at* https://www.javelinstrategy.com/uploads/files/1004.R_2010IdentityFraudSurveyConsumer.pdf.

[7] FTC DATA BOOK, supra note 5, at 3. While the Federal Trade Commission and most other U.S. governmental organizations consider credit card fraud to be a subset of a large category of identity theft crimes, some organizations and consumer advocacy groups use narrower definitions for the two terms, and consider the two categories of crimes to be separate. Other organizations use the terms identity theft and credit card fraud interchangeably. For purposes of clarity, this Comment will use the approach of the Federal Trade Commission as described in the main text.

[8] *Id.* at 11.

experience personal costs absorbed an average cost of $373 and spent an average of twenty-one hours resolving the fraud.[9]

¶8 The costs of credit card fraud to the economy as a whole are staggering. Industry analysts report that the total loss to the industry of credit card issuers due to credit card fraud in 2007 was approximately $1.04 billion.[10] However, this figure is only the beginning of the total cost of credit card fraud to the U.S. economy, as it encompasses only those fraudulent purchases where the credit card itself was actually present during the fraudulent purchase. Online merchants are estimated to lose approximately double that amount ($2.2 billion) each year as a result of fraudulent purchases where the credit card was not physically present, as the transaction took place via the Internet.[11]

¶9 Losses of an even greater magnitude stem from purchases that ultimately never take place as a result of the effects of credit card fraud. These losses are collectively referred to as lost card usage. The costs of lost card usage include legitimate transactions declined due to erroneous suspicion of fraud, lost volume of credit card purchases during the downtime between card cancellation and reissue, and consumers turning to alternative methods of payment, which they perceive as safer. Lost card usage is estimated to total approximately $5 billion in losses across credit card issuers and merchants.[12] Another estimated $7.5 billion in total costs affecting consumers stems from additional frauds and scams that prey on consumer fear of credit card fraud, including illegal and worthless "credit repair" services and unnecessary credit card insurance.[13]

¶10 The preceding costs and losses associated with credit card fraud total approximately $16 billion per year.[14] Even more costs of credit card fraud exist that are either intangible or impossible to aggregate at an economy-wide level, but are estimated to be even greater still. These include the indirect costs and mental anguish to consumers in repairing their personal situations, resources spent by law enforcement in investigating these crimes, and the legal expenses and damaged reputations of the affected credit card issuers and merchants.[15]

B. How Credit Card Fraud Occurs

¶11 In order to understand how federal legislation seeks to combat credit card fraud, it is first necessary to outline the most common ways in which credit card fraud is carried out. These include phishing, skimming, and low-tech methods such as the fraudulent use of lost or stolen cards, card copying, and dumpster-diving.

---

[9] JAVELIN STRATEGY & RESEARCH, *supra* note 6, at 5.
[10] KEN PATERSON, MERCATOR ADVISORY GRP., CREDIT CARD ISSUER FRAUD MANAGEMENT: REPORT HIGHLIGHTS 6 (2008), *available at* http://www.mercatoradvisorygroup.com/index.php?doc=Credit&action=view_item&id=325&catid=3.
[11] *Id.*
[12] *Id.* at 6–7.
[13] *Id.* at 7.
[14] *Id.*
[15] *Id.*

1. Phishing

¶12 Phishing occurs when an individual receives an e-mail or phone call from a seemingly legitimate source that is actually from a person or group which is attempting to obtain that individual's account information, password, or both.[16] For example, an individual may receive an e-mail that appears to have come from her bank or credit card company, stating that an important notice has been posted online and should be read immediately. The e-mail will often create a false sense of urgency by threatening that the individual's account may be suspended or closed if this action is not taken right away.[17] The e-mail looks very much like a legitimate e-mail the individual would receive from her financial institution, complete with the actual logo and similar formatting. However, when she clicks the included link to go sign-in to read the "important notice," she is actually directed to a fake website which, once again, has a very similar or even identical look and feel to the institution's actual website. When the individual attempts to sign in by entering her account information, it is recorded by the fake website. At that point, the perpetrators of the phishing attempt have all the information necessary to enter the victim's real financial account and use it to carry out a number of fraudulent activities, such as making new purchases, opening a new account in the victim's name, or transferring all the victim's funds to other accounts.[18]

¶13 Phishing schemes are also used to gather account information and passwords for e-mail sites such as Google's Gmail, and social networking sites such as Facebook.[19] Once the perpetrators have logged in to these sites using a victim's username and password, they can then search the site or e-mail archives for credit card numbers, financial account information, and other private information.

¶14 All major financial institutions let their users know that they will never ask for sensitive account information via e-mail, nor will they send any type of time-sensitive, urgent e-mails requesting that account information be updated or confirmed.[20] However, phishing attempts are still among the most frequent fraud attacks on consumers. The Anti-Phishing Working Group (APWG), a global law-enforcement association dedicated to combating phishing sites and educating users about these threats, received over 33,000 unique reports of phishing e-mails from consumers in June 2010 alone.[21] In June 2010, the APWG detected 32,279 unique phishing websites,[22] with the vast majority of those sites (almost 70%) hosted in the United States.[23] Cumulative losses from phishing were

[16] *Report Phishing*, U.S. COMPUTER EMERGENCY READINESS TEAM, http://www.us-cert.gov/nav/report_phishing.html (last visited Aug. 25, 2011).
[17] *E-mail Fraud & Security – Spot a Spoof*, CITIBANK, http://www.citibank.com/domain/spoof/spotspoof.htm (last visited Aug. 25, 2011).
[18] *Recognizing Credit Card Fraud*, CONSUMER ACTION (July 8, 2009), http://www.consumer-action.org/english/articles/recognizing_credit_card_fraud_english/.
[19] Thomas Claburn, *'Tabnapping' Attack Simplifies Phishing*, INFORMATIONWEEK (May 25, 2010, 6:01 PM) http://www.informationweek.com/news/software/showArticle.jhtml?articleID=225200157; Doug Gross, *Facebook Responds to Massive Phishing Scheme*, CNN SCITECHBLOG (Mar. 19, 2010 1:30 PM), http://scitech.blogs.cnn.com/2010/03/19/facebook-responds-to-massive-phishing-scheme/.
[20] *See*, *e.g.*, *E-mail Fraud & Security – Spot a Spoof*, *supra* note 17.
[21] ANTI-PHISHING WORKING GRP., PHISHING ACTIVITY TRENDS REPORT: 2ND QUARTER 2010, at 4 (2010), *available at* http://www.antiphishing.org/reports/apwg_report_q2_2010.pdf.
[22] *Id.*
[23] *Id.* at 7.

estimated to be $2.8 billion in 2006, and a Wall Street Journal poll found that 24% of respondents stated they limited their online banking transactions due to fear of such attacks.[24]

2. Skimming

¶15 Skimming occurs when a device is placed over the card-reader (on an ATM, for example), which duplicates the information embedded on the debit or credit card's magnetic strip.[25] Some devices are even more sophisticated and include a pinhole camera or false panel near the card-reader in order to track the user's entry of a personal identification number (PIN) on the attached keypad.[26] The perpetrators of the skimming operation can then retrieve their skimming device and encode these same magnetic strips onto entirely new cards, which they can then use for fraudulent purchases as if they had the victims' physical cards themselves.[27] These skimming operations have recently become even more refined, as wireless technology has made it possible for the magnetic strip information to be sent to the perpetrators wirelessly, so they do not even have to return to physically retrieve the skimming device.[28]

¶16 This method is particularly difficult for victims to protect against, as the false panels and skimming devices are constructed to appear very similar to the regular card readers and ATM panels they cover. Although users are encouraged to carefully inspect the devices they use and to use the more secure ATMs inside of banks whenever possible, the best protection users may have is to simply monitor their credit card transaction history on a regular basis and be on the lookout for any fraudulent charges, which they should then report to their financial institution immediately.[29]

¶17 Skimming is a lucrative scheme, and it is estimated that carrying out a skimming operation on a single ATM will yield an average of $50,000.[30] Bankrate.com estimates that the total yearly theft from skimming is approximately $1 billion,[31] and Javelin Strategy & Research[32] estimates that one out of every five people has been the victim of an ATM skimming operation.[33]

---

[24] *White Paper: Who Is Fighting Phishing?*, COMPUTERWEEKLY.COM (Oct. 26, 2010, 7:59 PM), http://www.computerweekly.com/Articles/2010/10/26/243551/White-paper-Who-is-fighting-phishing.htm.
[25] Jennifer Waters, *ATM Skimming: How to Spot, Avoid*, WALL ST. J., Oct. 10, 2010, at C17, *available at* http://online.wsj.com/article/SB10001424052748704442404575542652417958106.html.
[26] *Id.*
[27] *Id.*
[28] *BBB Warns that Debit and Credit Card Skimming Is on the Rise*, TUCSON CITIZEN (Nov. 1, 2010, 4:01 PM), http://tucsoncitizen.com/bbbconsumeralert/2010/11/01/bbb-warns-debit-and-credit-card-skimming-is-on-the-rise/.
[29] *Id.*
[30] Waters, *supra* note 25.
[31] Constance Gustke, *4 Tips to Protect You from ATM Thieves*, BANKRATE.COM (July 14, 2010), http://www.bankrate.com/finance/savings/4-tips-to-protect-you-from-atm-thieves-1.aspx.
[32] Javelin Strategy & Research is a research institution that conducts continuous quantitative research on topics pertaining to the financial services sector.
[33] Gustke, *supra* note 31.

3. "Old-Fashioned Theft": Stolen and Lost Cards, Copying, Receipts, and Dumpster-Diving

¶18 The oldest, and arguably the least sophisticated method of carrying out credit card fraud, is by stealing the actual card itself, through the theft of a wallet, purse, or even a home invasion. Some perpetrators may simply come across a lost card and decide to make fraudulent purchases before the owner realizes the card has been lost.[34] However, both of these incidents are of the highest visibility for victims, who will call to notify their financial institutions as soon as they are aware that their actual cards have been lost or stolen.

¶19 Other low-tech methods of fraud include copying sensitive information through what is referred to as "shoulder-surfing."[35] In this method, a perpetrator will eavesdrop on a telephone call where the victim is providing credit card information or will observe the oblivious victim entering a password or PIN onto an ATM keypad or making an online transaction on a laptop in a public area such as an Internet café or library.[36] Card information can also be copied by a dishonest cashier during any in-person transaction, as the credit card number, expiration date, and security code are all present on the victim's card.[37] Copying this information can be done quickly and discreetly due to the ubiquity of computers in today's stores.

¶20 A final low-tech method of carrying out credit card fraud is through the act of "dumpster-diving," where perpetrators will sift through dumpsters and trash bins outside businesses and residences to look for documents and discarded receipts that can divulge a variety of personal information, such as phone numbers, social security numbers, financial account numbers, and credit card numbers.[38]

¶21 A popular method of carrying out credit card fraud by this method occurs when the perpetrator finds a discarded pre-approved credit card offer along with the information necessary to activate the card in the victim's name.[39] Victims often do not think twice about throwing away these types of pre-approved offers, as well as bills, credit card statements, and bank statements. Shredding these types of documents offers a quick and

[34] *Recognizing Credit Card Fraud*, *supra* note 18.
[35] Tim Bates, *Protecting Yourself from Identity Theft*, ROME OBSERVER (Oct. 14, 2010), http://www.romeobserver.com/articles/2010/10/14/opinion/doc4cb7443d18891039275406.txt.
[36] *Id.*
[37] Security code, in this context, refers to an additional code, found today on most major credit cards, which is often required to make a card-not-present (e.g. online, over-the-phone) purchase. Different credit card issuers refer to it through a host of remarkably similar acronyms and names, such as Card Verification Value (CVV), Card Verification Code (CVC or CVC2), Card Code Verification (CCV), etc. This additional security measure helps to combat credit card fraud in cases where the perpetrator has only the card owner's name, credit card number, and expiration date off a receipt, as the security code is not usually printed on receipts. However, as discussed in this Comment, a variety of fraud methods are able to procure this code, so it is by no means a perfect safeguard. *See, e.g.*, *Security Features*, VISA, http://www.visa.ca/en/merchant/pdfs/security_features.pdf (last visited Aug. 25, 2011).
[38] *About Identity Theft*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last visited Aug. 25, 2011).
[39] *What to Shred*, WASHINGTON STATE OFFICE OF THE ATT'Y GEN., http://www.atg.wa.gov/page.aspx?id=13148 (last visited Aug. 25, 2011).

easy way to prevent dumpster divers from finding usable information,[40] but, while many corporations use such devices, few people use them at their private residence.

C. E-mail Security Concerns

¶22 The rise of the Internet has brought a new venue to perpetrators of identity theft and credit card fraud. A 2009 survey found that 47% of respondents used online banking services.[41] While this has contributed to the rise in phishing attacks, it also creates new security concerns, as individuals store banking statements, credit card purchase receipts, and account number and password reminders in their e-mail inboxes and archives. As Drew Voros, Business Editor of the Oakland Tribune, aptly stated: "Today's Dumpster is the Internet, and the amount of personal information that litters the information superhighway is incredible."[42] As more and more people become familiar with e-mail and sign up for personal accounts, the amount of e-mail accounts being hacked is at an all-time high. A recent FBI report states that 336,655 complaints regarding e-mail account theft and other online fraud attempts were filed to its Internet Crime Complaint Center in 2009, representing a 22.3% increase over 2008.[43] Making e-mail account hacking even more difficult to combat is the fact that anyone, anywhere can access the most popular personal e-mail services, such as Gmail, Yahoo, and Hotmail, and that younger users are particularly tech-savvy. A March 2010 study by the Association of Chief Police Officers (ACPO) in the United Kingdom reported that 26% of college students had hacked into someone else's e-mail account and that 46% had experienced one of their own accounts being compromised.[44]

¶23 The rise in online purchases has led many online vendors to provide e-mail confirmations and receipts in lieu of paper receipts. Just as many individuals store paper receipts in their homes in case a product proves to be defective, these e-mail confirmations and receipts can be stored in the inboxes of consumers for years at zero cost to them. E-mail providers such as Google have an "archive" function, which allows users to reduce clutter in their inboxes, but retain important e-mails, such as receipts and purchase confirmations, indefinitely.[45] Gmail's built-in search feature is particularly useful for finding a particular e-mail in the annals of one's e-mail account, but unfortunately makes it very easy for someone who has hacked an e-mail account to quickly find sensitive account and credit card information through this same function.[46]

---

[40] *Id.*

[41] Lance Whitney, *Online Banking Is Booming*, CNET NEWS (June 16, 2009, 8:59 AM), http://news.cnet.com/8301-1001_3-10265409-92.html.

[42] Drew Voros, *Your Online Privacy Slips Through Web's Cracks*, SILICON VALLEY MERCURY NEWS, http://www.mercurynews.com/columns/ci_16378229?nclick_check=1 (last visited Oct. 20, 2010).

[43] Linda Finarelli, *Identity Theft Is on the Rise in Montgomery County, but There Are Deterrents*, AMBLER GAZETTE (Oct. 29, 2010), http://www.montgomerynews.com/articles/2010/10/29/ambler_gazette/news/doc4cc85d96b71a2480954809.txt.

[44] Claire West, *One in Five College and University Students Have Hacked*, FRESHBUSINESSTHINKING.COM (Sept. 21, 2010), http://www.freshbusinessthinking.com/news.php?CID=4&NID=6185&Title=One+in+five+college+and+university+students+have+hacked.

[45] *Archive Mail*, GOOGLE GMAIL HELP, http://mail.google.com/support/bin/answer.py?hl=en&answer=6576 (last updated July 28, 2011).

[46] *Searching Mail*, GMAIL HELP, http://mail.google.com/support/bin/static.py?page=guide.cs&guide=21758&topic=21766 (last visited Aug. 25, 2011).

An alarming recent example of credit card information being compromised through an e-mail receipt stemmed from an error in order confirmation e-mails sent from the catalogue company Argos. A customer who checked the source code of an Argos order confirmation e-mail discovered that his full credit card number and security code were present in the code.[47] If any Argos customer receiving such an e-mail were to find his e-mail account compromised, the perpetrator would only have to do a quick search to find this information and begin making fraudulent purchases.

¶24 While e-mail receipts and confirmations from online vendors have become the standard, and consumers do have good reason to retain these e-mails, consumers should be increasingly concerned with the security of their e-mail accounts and should frequently change their passwords and protect them appropriately to minimize the risk of becoming a victim of this form of credit card fraud.

FCRA AND FACTA: LEGISLATION DESIGNED TO ENSURE FAIRNESS IN CREDIT REPORTS AND COMBAT IDENTITY THEFT

¶25 The Fair Credit Reporting Act (FCRA)[48] was passed in 1970 in part "to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy."[49] FCRA was designed to address concerns that consumer credit reports, if allowed to remain secret (existing solely in the hands of consumer reporting agencies), could contain errors that would adversely affect consumers regarding their ability to acquire credit and consumers would have no chance for correction.[50] As such, FCRA mandates that all consumer reporting agencies "maintain reasonable procedures" to avoid inaccuracies in consumer reports, and that the consumer be notified upon the preparation of an investigative consumer report on his or her person.[51] FCRA's scope was thereby limited to the procedures followed by consumer reporting agencies, ensuring that the information contained in their reports was as accurate as possible. However, as identity theft increasingly affected U.S. consumers through the early 1990s, critics of the Act were concerned that FCRA did very little, if anything, to prevent these crimes.[52]

¶26 The Fair and Accurate Credit Transactions Act (FACTA) was passed in 2003 to address such concerns.[53] Several provisions within FACTA are specifically intended to combat identity theft and empower consumers to better monitor their credit and financial situations. Recognizing the benefits of self-monitoring, Congress included within FACTA a provision that allows consumers to request one credit report annually from each of the three major credit report agencies (Equifax, Experian, and TransUnion), free

---

[47] John Leyden, *Argos Buries Unencrypted Credit Card Data in Email Receipts*, THE REGISTER (Mar. 5, 2010 11:49 GMT), http://www.theregister.co.uk/2010/03/05/argos_email_security_snafu/.
[48] Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x (2006).
[49] *Id.* § 1681(a)(4).
[50] *Id.* § 1681i(a)(1)(A).
[51] *Id.* §§ 1681d, 1681e.
[52] Brandon McKelvey, Comment, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft*, 34 U.C. DAVIS L. REV. 1077, 1091 (2001) ("The limited protection of . . . the FCRA has proved insufficient to prevent identity theft.").
[53] Fair and Accurate Credit Transaction Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. § 1681 (2006)).

of charge.[54] The website www.annualcreditreport.com was established for this purpose, though consumers still have the option to request their free credit reports via telephone or mail.[55] This provision allows consumers, at no charge, to review their credit report and credit score each year to ensure that no fraudulent accounts or activity are present.

¶27 Another FACTA provision intended to empower consumers in the fight against identity theft pertains to the creation of fraud alerts.[56] Essentially, consumers who believe they may be at risk of becoming a victim of fraud or identity theft may "flag" their credit files. Consumers are then notified of any new credit activity while the alert is in place, and the business receiving the credit request is required to take "reasonable steps" to ensure that the request is not being made by an identity thief.[57] FACTA also mandates that consumers be allowed to block any negative information on their credit reports that resulted from fraud or identity theft.[58] These provisions provide consumers with the opportunity to receive immediate knowledge of any activity on their credit report and increase their ability to ensure that the information on their credit report is accurate. Furthermore, FACTA includes a mandatory procedure for businesses to follow when disposing of consumer credit reports.[59]

¶28 The FACTA provision most pertinent to the discussion in this Comment is the credit card number truncation requirement for receipts. The provision states 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."[60] This provision is limited to "apply only to receipts that are electronically printed," with handwritten receipts and credit card imprints specifically excluded.[61] This truncation requirement was specifically intended to protect consumers from the likes of dumpster divers and other would-be perpetrators of identity theft and credit card fraud by making it more difficult to obtain discarded receipts that contain a card owner's entire credit card number and expiration date.[62]

¶29 To enforce these provisions, FACTA provides that a plaintiff who proves a willful violation of any FACTA provision is entitled to recover the cost of litigation, attorney's fees, punitive damages, and actual damages or statutory damages of "not less than $100

---

[54] 15 U.S.C. § 1681j.
[55] *About Us*, ANNUALCREDITREPORT.COM, https://www.annualcreditreport.com/cra/helpabout (last updated Mar. 30, 2010).
[56] 15 U.S.C. § 1681c-1.
[57] *Id.*
[58] *Id.* § 1681c-2.
[59] *Id.* § 1681w.
[60] *Id.* § 1681c(g)(1).
[61] *Id.* § 1681c(g)(2).
[62] *See* Iosello v. Leiblys, Inc., 502 F. Supp. 2d 782, 786 (N.D. Ill. 2007) ("Congress enacted FACTA with the intent of helping to prevent the possibility of thieves stealing the identity of another by obtaining one's credit card number and the expiration date of that credit card. Businesses generally require one's credit card number and the expiration date of that credit card to transact business. Access to both the credit card number and the expiration date of that credit card makes it easier for a thief to commit identity theft. The existence of a law prohibiting the printing of more than the last five digits of the credit card number makes it difficult for a thief to obtain the victim's credit card number. The existence of a law prohibiting the printing of the expiration date of a credit card makes it even more difficult to commit identity theft.").

and not more than $1,000."[63] FACTA does not cap the total damages that can be recovered by a class action lawsuit. This means that a large company could be forced to pay an enormous amount of damages if its stores do not update their receipt process. Immediately after FACTA went into effect, "hundreds of lawsuits" were filed by consumers seeking to enforce the truncation requirement against businesses that were not in compliance.[64]

¶30 Many of these lawsuits were filed because, although the merchant properly truncated the consumer's credit card number, the expiration date was included on the receipt. However, a significant number of merchants believed this was in compliance with FACTA's truncation requirement due to the provision's ambiguous wording.[65] As a result of this ambiguity, Congress passed the Credit and Debit Card Receipt Clarification Act of 2007, which limits liability for those merchants who mistakenly included the expiration date since the enactment of FACTA and clarifies that any future inclusions of the expiration date on a receipt will constitute a violation.[66]

¶31 Unfortunately, this is not the only ambiguity presented by FACTA's truncation requirement. As discussed in Part I of this Comment, e-mail confirmations and receipts have seemingly become standard issue for online purchases, and the ever-present threat that e-mail accounts will be hacked or otherwise compromised makes e-mail confirmation receipts, which include full credit card numbers and other sensitive information, hazardous to retain. But do such e-mails fall under FACTA's truncation requirement? Are e-mails, viewed solely on a computer screen, considered "electronically printed"? In the recent case *Shlahtichman v. 1-800 Contacts*, the Seventh Circuit was charged with answering exactly this question.

SHLAHTICHMAN V. 1-800 CONTACTS: THE SEVENTH CIRCUIT HOLDS FACTA DOES NOT APPLY TO E-MAIL CONFIRMATIONS OR RECEIPTS

¶32 On June 2, 2009, plaintiff Eduard Shlahtichman went online and purchased contact lenses with his credit card at the website of defendant 1-800 Contacts, a corporation that sells contact lenses over the Internet.[67] The same day, Shlahtichman received an automatically generated e-mail receipt of the purchase, which included the expiration date of his credit card.[68] Shlahtichman filed suit, alleging that 1-800 Contacts had committed a willful violation of FACTA's truncation requirement and seeking statutory damages.[69] 1-800 Contacts moved to dismiss the complaint for failure to state a claim on

---

[63] 15 U.S.C. § 1681n(a).
[64] Michael E. Chaplin, *What's So Fair About the Fair and Accurate Credit Transactions Act?*, 92 MARQ. L. REV. 307, 311–12 (2008).
[65] Credit and Debit Card Receipt Clarification Act of 2007, Pub. L. No. 110-241, § 2(a)(3), 122 Stat. 1565.
[66] Chaplin, *supra* note 64, at 313 ("In effect, the Clarification Act gives merchants one free bite at the apple. That is, the law appears to say: 'Okay, you were wrong, but we won't count it against you—just don't do it again.'").
[67] Shlahtichman v. 1-800 Contacts, Inc., No. 09 CV 4032, 2009 U.S. Dist. LEXIS 112379, at *1 (N.D. Ill. Dec. 2, 2009).
[68] *Id.* at *1–2.
[69] *Id.* at *2. Shlahtichman initially filed suit in Illinois state court, but on July 6, 2009, the complaint was removed to federal court. It is worth noting that Shlahtichman, like the vast majority of plaintiffs filing suit due to an alleged violation of FACTA's truncation requirement, did not allege that any actual harm in the

which relief could be granted, asserting that FACTA does not apply to e-mail confirmations, because such e-mails are not "electronically printed" receipts under FACTA and are also not provided "at the point of the sale or transaction" as understood under FACTA.[70]

A. The District Court's Holding

¶33 The district court ultimately agreed with 1-800 Contacts' assertions, and held that e-mail confirmations are neither "electronically-printed" receipts, nor are they provided "at the point of sale or transaction" under the meaning of FACTA.[71] In reaching its decision that e-mail confirmations are not electronically printed, the district court looked to past court decisions on the same issue and found that a majority held that e-mail confirmations are not printed receipts under FACTA.[72] The district court also stated that, in the absence of a statutory definition (no such definition for "print" is present in the text of FACTA), a court should look to a term's plain meaning and found that several dictionaries defined "print" as "the process of transferring information to paper."[73] This definition precludes the term "print" from encompassing e-mail confirmations like the one Shlahtichman received. Shlahtichman also offered that the term "print" is also commonly used to mean "to display on a surface (as a computer screen) for viewing," but the district court found this argument to be unpersuasive.[74] The district court cited one court's particularly strong argument to the contrary as further support:

> "In sum, the word 'print' does not encompass onscreen computer displays because 'print' only refers to a tangible, paper receipt. That is why Mr. Grabein had to print a copy of his receipt to get it off of his computer; it is why the machine used to transfer text from a computer to paper is called a printer; and it is why a judge who asks a law clerk to print a case does not intend for the clerk to merely display the case on his computer screen."[75]

¶34 Shlahtichman also contended that the text of FACTA intended to include computers receiving e-mails like this, as FACTA refers to "the date that 'any cash register or *other machine or device* that prints receipts for credit card or debit card transactions' is put into use."[76] However, the district court disagreed, citing the "statutory interpretation rule of *ejusdem generis*," which states that "when a statute sets out a specific term and a general term, the general term is confined to covering subjects

---

form of credit card fraud or identity theft took place as a result of the e-mail he received from 1-800 Contacts. However, as discussed in Part III of this Comment, a showing of actual harm is not necessary for a plaintiff to recover the statutory damages outlined in FACTA. For an in-depth (and enjoyable) discussion of the potential societal harms brought about by FACTA's construct of awarding statutory damages without a showing of actual harm, read Chaplin, *supra* note 64.

[70] *Shlahtichman*, 2009 U.S. Dist. LEXIS 112379, at *2, *5.

[71] *Id.* at *7.

[72] *Id.*

[73] *Id.* at *10–11.

[74] *Id.* at *11.

[75] *Id.* at *12 (quoting Grabein v. Jupiterimages Corp., No. 07-22288-CIV, 2008 U.S. Dist. LEXIS 65828, at *22–23 (S.D. Fla. July 7, 2008)).

[76] *Id.* at *12–13; 15 (emphasis added) (quoting U.S.C. § 1681c(g)(3) (2006)).

comparable to the specifics it follows."[77] In this case, the district court reasoned, the other machines FACTA refers to must be "devices akin to cash registers," such as point-of-sale terminals.[78] The district court felt that home computers were too dissimilar to be included in this language.[79]

¶35 The district court also looked to the legislative history of FACTA and found that Congress enacted FACTA as a means of combating low-tech methods of identity theft such as dumpster diving, which is an activity associated with the search for discarded physical receipts, not e-mails.[80] Although Shlahtichman proffered two committee reports, which "recognize that the Internet can facilitate identity theft," the district court did not feel this was enough to show that FACTA was intended to cover e-mail confirmations and receipts.[81]

¶36 1-800 Contacts' second assertion was that e-mails like the one sent to Shlahtichman are not receipts provided "at the point of sale or transaction" as understood under FACTA, and again, the district court agreed.[82] The district court cited prior decisions in which it was held that, in context, the language of FACTA contemplates a transaction wherein the customer is physically present and receives a "tangible, paper" receipt.[83] Although Shlahtichman argued that, in the case of an online purchase, the point of sale is at whatever computer or other device the consumer makes said purchase, the district court did not agree.[84] The district court held that FACTA did not contemplate online purchases, because, in the context of such a purchase, the phrase "point of sale or transaction" does not make sense and e-mails like the one Shlahtichman received are not directed to any particular computer in any particular location, but are instead "provided to an account, which can be accessed anywhere in the world."[85]

¶37 Thus, the district court reasoned that the order confirmation e-mail that Shlahtichman received did not fall under the protection of FACTA and granted 1-800 Contacts' motion to dismiss.[86]

B. The Seventh Circuit Affirms

¶38 Shlahtichman appealed the district court's decision, and the case was argued before the United States Court of Appeals for the Seventh Circuit on April 15, 2010 and was ultimately decided on August 10, 2010.[87] The court noted that the question of whether 1-800 Contacts had electronically printed the expiration date of Shlahtichman's credit card

---

[77] *Id.* at *12–13.
[78] *Id.* at *13.
[79] *Id.*
[80] *Id.* at *14; *see also The Fair Credit Reporting Act and Issues Presented by Reauthorization of the Expiring Preemption Provisions: Hearings Before the S. Comm. on Banking, Hous., and Urban Affairs*, 108th Cong. 78 (2003) ("In other words, the receipt, the part you discard, does not show the whole number on there so people cannot go into the garbage can, pick it up, and duplicate your credit card number.") (statement of Sen. Charles E. Schumer).
[81] *Shlahtichman*, 2009 U.S. Dist. LEXIS 112379, at *15.
[82] *Id.* at *16.
[83] *Id.* at *16–17.
[84] *Id.* at *17.
[85] *Id.* at *17–18.
[86] *Id.* at *18.
[87] Shlahtichman v. 1-800 Contacts, Inc., 615 F.3d 794 (7th Cir. 2010).

in its e-mail confirmation, thereby violating FACTA, was a question of first impression at the federal appellate level.[88]

¶39 The court first examined 1-800 Contacts' assertion that e-mails like the one Shlahtichman received are not "electronically printed" under FACTA and agreed with the district court's holding that such e-mails are not protected by FACTA.[89] Like the district court before it, the court considered that the majority of prior decisions at the district court level also agreed with this assertion and looked to dictionaries to determine that the ordinary meaning of the term "print" meant to "transfer of words or images to a tangible medium—often paper."[90] Although the court recognized that some dictionaries included Shlahtichman's alternate definition of "to display on a surface (as a computer screen) for viewing," the court reasoned that this definition does "not yet represent the ordinary or natural meaning of 'print.'"[91] Shlahtichman's additional argument that the inclusion of the word "electronically" suggests intent to encompass future technologies such as e-mails was met with the court's reasoning that it was instead "intended to distinguish those receipts that are printed by machine, as opposed to those which are handwritten or created by taking an impression of the card using an imprinter."[92]

¶40 The court also agreed with the district court's reasoning regarding 1-800 Contacts' second assertion that e-mails are not provided "at the point of sale or transaction."[93] It echoed the reasoning that FACTA's language contemplates a face-to-face transaction where a consumer is handed a physical receipt, and that no tangible "point of sale or transaction" exists for an Internet purchase.[94]

¶41 The court went on to say that FACTA's "statutory language strikes us as significant not only for the terms that it uses but for those it does not," pointing out that U.S. consumers were quite familiar with e-commerce when FACTA was enacted in 2003, as Internet retail sales "reached $56 billion in the United States that year."[95] And yet, the court continued, Congress made no specific mention of the Internet or e-mails in the text of FACTA to ensure that they fall within its scope, despite having explicitly done so in the past in the text of other statutes.[96] The court then cited several statutes in which Congress had specifically included electronic media and transactions to support this contention.[97]

¶42 Finally, the court acknowledged that, although FACTA's truncation requirement was a provision enacted to prevent identity theft, the language of FACTA was too clear in limiting its scope to printed receipts, and it was therefore unable to extend it to e-mails like Shlahtichman's.[98] The court effectively slammed the door on e-mails falling under FACTA protection by stating:

---

[88] *Id.* at 796.
[89] *Id.* at 798.
[90] *Id.* at 798–99.
[91] *Id.* at 799.
[92] *Id.*
[93] *Id.* at 800.
[94] *Id.*
[95] *Id.* at 801.
[96] *Id.*
[97] *Id.* at 801–02.
[98] *Id.* at 802.

¶43 Both the language and context of the truncation requirement make plain that Congress was regulating only those receipts physically printed by the vendor at the point of the sale or transaction; to apply the statute to receipts that are emailed to the consumer would broaden the statute's reach beyond the words that Congress actually used.[99]

¶44 The court recognized that e-mail confirmations and receipts can still pose a risk of consumers becoming victims of identity theft and credit card fraud if the credit card numbers therein are not also properly truncated. However, the court further opined that, while paper receipts and e-mail receipts each pose "unique" dangers in this regard, paper receipts, since they can be physically lost or discarded, pose an arguably greater risk.[100] The court further justified its holding by stating that Congress may have simply thought that the risks posed by e-mail confirmations and receipts were "better addressed by other statutory provisions" specific to this technology.[101]

¶45 Ultimately, the court affirmed the judgment of the district court, and Shlahtichman's battle for statutory damages was over.[102]

CONGRESS SHOULD AMEND FACTA TO SPECIFICALLY INCLUDE E-MAIL RECEIPTS AND CONFIRMATIONS

¶46 As discussed in Part I-C of this Comment, there clearly exists a genuine risk to consumers that financial account information such as credit card numbers and passwords, if present in their inboxes, will be stolen due to the unrelenting threat of their e-mail accounts being hacked. However, the holding in *Shlahtichman* unambiguously states that e-mail confirmations and receipts do not fall under the protection of FACTA. The problem this situation creates is clear. E-mail receipts and confirmations from online merchants can contain the full credit card number and expiration date of consumers, and FACTA offers those consumers no recourse.

¶47 Although the Supreme Court could potentially grant certiorari and hold that FACTA and its truncation requirement do, in fact, apply to e-mail receipts and confirmations, this seems highly unlikely. The Seventh Circuit's holding is well-supported given the clear plain meaning of the term "electronically print," the fact that the vast majority of district courts held that "electronically print" does not apply to e-mails,[103] the context and language of FACTA as a whole, the legislative history of FACTA suggesting it was enacted as a means of curbing low-tech identity theft, and the

---

[99] *Id.*
[100] *Id.* at 802–03.
[101] *Id.* at 803.
[102] *Id.* at 804.
[103] In the few district court cases in which courts held that the term "electronically print" did, in fact, apply to e-mail receipts, the courts felt that the alternate definition of "print" of "to display on a surface (as a computer screen) for viewing" being present in a dictionary was enough to include that within the everyday meaning of the term. The courts either did not consider the other factors stated here (overall context and language of FACTA, legislative history, and omission of e-commerce terms) to be as important as did the vast majority of courts approaching this issue, or did not consider them at all. *See, e.g.*, Romano v. Active Network, Inc., No. 09 C 1905, 2009 U.S. Dist. LEXIS 78983 (N.D. Ill. Sept. 3, 2009); Harris v. Best Buy Co., 254 F.R.D. 82 (N.D. Ill. 2008); Grabein v. 1-800-Flowers.com, Inc., No. 07-22235-CIV, 2008 U.S. Dist. LEXIS 11757 (S.D. Fla. Jan. 29, 2008); Vasquez-Torres v. Stubhub, Inc., No. CV 07-1328, 2007 U.S. Dist. LEXIS 63719 (C.D. Cal. July 2, 2007).

resounding omission of any terms reflecting an intent for FACTA to apply to e-commerce. All these factors suggest that the Seventh Circuit correctly decided the case given the current wording and background of FACTA.

¶48 Therefore, to rectify this situation, Congress should further its stated goal within FACTA of combating identity theft by amending FACTA to specifically include e-mail confirmations and receipts within its scope. This would require merchants to truncate their customers' credit card numbers and remove credit card expiration dates from these e-mails as they currently must do for paper receipts.

¶49 Finding concrete evidence regarding the relative magnitude of the fraud-related risks posed by paper and e-mail receipts is problematic at best, largely due to the difficulties associated with collecting such data and tracking these crimes. In *Shlahtichman*, the Seventh Circuit suggested the risk posed by paper receipts is arguably greater than that of e-mailed receipts and confirmations, since paper receipts can be dropped, mislaid, or retrieved from the trash, and e-mail receipts are typically only viewed on a computer screen and are thus less subject to inadvertent disclosure.[104] However, this does not discount the fact that there undoubtedly exists a very real and tangible risk to consumers if e-mail receipts and confirmations are not held to FACTA's truncation requirement, especially given the potential for such e-mails to exist in the e-mail account inboxes of consumers indefinitely. As discussed in Part I-C of this Comment, e-mail receipts containing credit card information can be located in a matter of seconds using the sophisticated search functions that are now present in almost all major e-mail services, which only increases the risk consumers face.

¶50 Amending FACTA as previously described would likely be met with little industry opposition, since revising the programming code which generates these automatic e-mail receipts and confirmations is a cheap and easy procedure for online businesses to undertake.[105] For some online merchants, the process would be as simple as a free software download from their merchant services provider.[106] This is further evidenced by the fact that some businesses have chosen to voluntarily truncate consumer credit card numbers on e-mail receipts and order confirmations just as they would if they were paper receipts. While this is certainly a welcome step in the right direction, the existence of recent cases like *Shlahtichman* shows that not all online businesses have elected to do so. Amending FACTA to specifically include e-mail receipts and confirmations under its protection will ensure that all online businesses take this simple, but important, step in advancing what is, after all, the Act's ultimate goal—protecting consumers from becoming victims of credit card fraud and identity theft.

CONCLUSION

¶51 Identity theft and credit card fraud are on the rise, not only in the United States, but worldwide, and consumers are at constant risk of falling victim to increasingly sophisticated methods of conducting fraud. The overwhelming cost that identity theft and credit card fraud pose to consumers and the worldwide economy are staggering, and,

---

[104] *Shlahtichman*, 615 F.3d at 802–03.
[105] *See, e.g.*, *Account Truncation Law*, MERCHANT SOURCE, http://www.merchantsource.com/truncation.html (last visited Aug. 25, 2011).
[106] *Id.*

while legislation like FACTA contains provisions which empower consumers to better monitor their credit and identify fraud sooner, this legislation must continue to evolve as technological advances continue to make it easier for perpetrators of identity theft and fraud to target victims.

¶52 The credit card truncation requirement within FACTA was an important step in removing discarded and lost credit card receipts from the arsenal of weapons that perpetrators of fraud have at their disposal. The *Shlahtichman* case was one of first impression at the appellate level, and its holding is clear: FACTA's truncation requirement does not apply to e-mail receipts and confirmations. In today's increasingly global world, where people are online more than ever and e-mail use continues to grow, this holding keeps the door wide open to the real risk of perpetrators of identity theft and credit card fraud seeking account information through compromised e-mail accounts.

¶53 The majority of courts faced with this issue have reached the same conclusion, and the overall language, context, and legislative history of FACTA suggest that the Seventh Circuit correctly decided *Shlahtichman*. Thus, it seems unlikely that a Supreme Court decision would come out the other way. The onus is on Congress to acknowledge the serious risk posed by leaving e-mails outside of FACTA's protection and to amend FACTA to specifically include e-mail receipts and confirmations within its scope. For online merchants, adhering to the new requirement will be quick and easy and will come at little to no cost. And those same online merchants, law enforcement, the credit industry, the worldwide economy, and, most importantly, consumers, will experience the benefits.