

1-1-2015

Riders on the Storm: An Analysis of Credit Card Fraud Cases

Ioana VasIU

Suffolk University Law School

Lucian VasIU

Suffolk University Law School

Follow this and additional works at: <https://dc.suffolk.edu/jtaa-suffolk>



Part of the [Litigation Commons](#)

Recommended Citation

20 Suffolk J. Trial & App. Advoc. 185 (2015)

This Article is brought to you for free and open access by Digital Collections @ Suffolk. It has been accepted for inclusion in Suffolk Journal of Trial and Appellate Advocacy by an authorized editor of Digital Collections @ Suffolk. For more information, please contact dct@suffolk.edu.

RIDERS ON THE STORM: AN ANALYSIS OF CREDIT CARD FRAUD CASES

Ioana Vasii and Lucian Vasii*

TABLE OF CONTENTS

I. INTRODUCTION.....	186
II. LEGAL ELEMENTS.....	191
A. Intent To Defraud.....	192
B. Access Device.....	195
C. Conspiracy And Extraterritorial Application.....	198
III. PERPETRATION ASPECTS.....	198
A. Virtual Obtaining Of Cards.....	199
B. Physical Obtaining Of Cards.....	205
C. Abuse Of A Position Of Trust.....	208
IV. SENTENCING ENHANCEMENTS.....	209
A. Amount Of Loss.....	210
B. Number Of Victims.....	212
C. Sophisticated Means.....	213
D. Role In The Offense.....	215
E. Upward Adjustments.....	216
V. CONCLUSION.....	217

Credit card fraud presents an impressive array of forms and methods, often involving sophisticated means, organized crime aspects, and

* Contact author: Prof. Dr. I. Vasii, Faculty of Law, Babeş-Bolyai University, e-mail: ioanav3@yahoo.com. She was partner and lead researcher on several international projects, funded by the European Commission or other entities: the FP7 Consent: Consumer Sentiment Regarding Privacy on User Generated Content Services in the Digital Economy (2010–2013); Rights of the Defense in Fraud Investigations (2004–2005); Grotius II (Criminal); and Provision of Information by Courts and Court Administrations: A Comparative Inventory of Eight European Countries and the USA. She chaired three major international Conferences, worked as expert for the UNDP Romania, has spoken at numerous professional events, and published widely on computer crimes. This article is part of a large-scale research on computer crimes, including *Break on Through: An Analysis of Computer Damage Cases*, 14 PGH. J. TECH. L. & POL'Y 158 (2014) and other forthcoming pieces. We give special thanks to Mr. Joseph McCarthy and the editors of the SUFFOLK JOURNAL OF TRIAL AND APPELLATE ADVOCACY for their very helpful edits and comments.

very significant criminal proceeds. Based on an extensive inquiry that involved the study of a large number of credit card fraud cases brought to the United States federal courts in violation of 18 U.S.C. § 1029(a)(1)-(5), press releases from law enforcement organizations, and information security reports, this article discusses the legal elements, the essential perpetration aspects, and the most relevant sentencing enhancements for these crimes, and proposes a number of improvements. The contributions of this article can be used for a more effective legal and judicial response in the process of risk identification and mitigation, and for developing awareness and training programs. Although the article focuses on one jurisdiction, the findings, particularly those in the perpetration aspects section, and the conclusion would be useful to a global audience.

I. INTRODUCTION

There is a large variety of electronic payment (“e-payment”) systems, such as ACH credit, debit, and on-us payments; wire transfers over Fedwire and CHIPS; and card payments.¹ The main benefits of electronic payments can be outlined as reduced transaction costs and payment collection,² increasing the transparency of payments,³ macroeconomic efficiency, expanded consumer markets and banking penetration, and increased capital turnover ratio.

Credit cards,⁴ despite the availability of a variety of electronic alternatives, such as digital wallets,⁵ checkout services,⁶ or virtual

¹ See *The 2013 Federal Reserve Payments Study*, FEDERAL RESERVE SYSTEM 63-76 (2014), https://www.frbservices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detail_ed_rpt.pdf (listing many potential choices for electronic payments); *Payment Systems in the United States*, BANK FOR INTERNATIONAL SETTLEMENTS, at 439-440 (2003), <http://www.bis.org/cpmi/paysys/unitedstatescomp.pdf> (discussing payment options for consumers).

² See David B. Humphrey & Robert Hunt, *Cost Savings from Check 21 Electronic Payment Legislation*, 45 JOURNAL OF MONEY, CREDIT AND BANKING 1415 (2013) (describing benefits of electronic payments).

³ See *The Opportunities of Digitizing Payments*, THE WORLD BANK (2014).

⁴ See 15 U.S.C. 1602(l) (defining credit card as “any card, plate, coupon book or other credit device existing for purpose of obtaining money, property, labor, or services on credit”); 15 U.S.C. § 1602(f) (defining credit as “the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment”).

⁵ See APPLE PAY, <https://www.apple.com/apple-pay/>, (last visited April 26, 2015), (providing contactless technology, which stores payment card data and requires, for making purchases, user’s finger, instead of passwords, for the authentication of user’s identity).

⁶ See PAYPAL, <https://www.paypal.com/>, (last visited April 26, 2015).

currencies,⁷ remain a widely used payment method.⁸ In the United States (“U.S.”), in 2012, the number of credit cards in force was about 333.6 million, the number of payments reaching 23.7 billion, for a total value of \$2.2 trillion.⁹ This situation is due to the interplay of numerous factors, such as the potential controlling of the timing of the repayment; the benefits of the reward programs offered; the large merchant-acceptance base; and the greater protection afforded to buyers than traditional payment mechanisms, because of the rights provided by Federal Reserve Regulation Z.¹⁰ This impressive usage, however, presents abundant criminal opportunities.

Although there are significant efforts¹¹ and innovations,¹² aiming to

⁷ See BITCOIN, <https://bitcoin.org/en/>, (last visited April 26, 2015); see also Stephanie Lo & J. Christina Wang, *Bitcoin as Money?*, FEDERAL RESERVE BANK OF BOSTON, No. 14-4 (2014); Lawrence Trautman, *Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014); Matthew Kien-Meng Ly, *Coining Bitcoin's “legal-bits”: Examining the regulatory framework for Bitcoin and virtual currencies*, 27 HARV. J.L. & TECH. 587 (2014); Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L.J. 159 (2012).

⁸ See Scott Schuh & Joanna Stavins, *How Consumers Pay: Adoption and Use of Payments*, FEDERAL RESERVE BANK OF BOSTON, 6-7 (2011), <http://www.bostonfed.org/economic/wp/wp2012/wp1202.pdf> (declaring credit cards the most popular form of payment other than cash). The United States Codes defines as credit card as “any card, plate, coupon book or other credit device existing for purpose of obtaining money, property, labor, or services on credit” and credit as “the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment”. 15 U.S.C. § 1602(l) (defining credit card); 15 U.S.C. § 1602(f) (defining credit). One digital wallet application that has recently gained notoriety is Apple Pay. See, e.g., APPLE PAY, <http://www.apple.com/apple-pay> (last visited Apr. 24, 2015). The most popular and nearly monopolistic checkout service is PayPal. See PAYPAL (<http://www.paypal.com>) (last visited Apr. 24, 2015) (exemplifying what constitutes a checkout service). With BitCoin's meteoric rise, the discussion of virtual currencies has recently expanded. See, e.g., Matthew Kien-Meng Ly, *Coining Bitcoin's “Legal-Bits”: Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV. J.L. & TECH. 587, 588-89 (2014) (explaining Bitcoin and virtual currencies).

⁹ See *The 2013 Federal Reserve Payments Study*, *supra* note 1, at 64-66 (displaying prevalence of credit cards in the modern economy).

¹⁰ See *Consumer Compliance Handbook*, THE FEDERAL RESERVE BOARD 1 (2014), available at <http://www.federalreserve.gov/boarddocs/supmanual/cch/tit.pdf> (presenting laws that primarily govern consumer transactions); see also Brianna L. Reed, *Mobilizing Payments: Behind the Screen of the Latest Payment Trend*, 14 J. HIGH. TECH. L. 451, 452-54 (2014) (explaining recent proliferation of mobile payments); Kevin V. Tu, *Regulating the New Cashless World*, 65 ALA. L. REV. 77, 82-84 (2013) (acknowledging increased alternate payment methods but recognizing domination of market by credit card companies).

¹¹ See, e.g., *Form 10-K*, VISA Inc., *Form 10-K* (Annual Report) Filed 11/21/14 for the Period Ending 09/30/14, at 24; American Express Company, *Form 10-K* For the fiscal year ended December 31, 2014.

¹² See, e.g., Scott C. Harris, *Intelligent Credit Card System*, U.S. Patent No. 20,150,095,226 (2 Apr. 2015); Kenneth Carnesi Sr., *EyeWatch credit card fraud prevention system*, U.S. Patent No. 20,150,100,493 (9 Apr. 2015); Jeffrey A. Aaron & John P. Ruckart, *User Terminal Location Based Credit Card Authorization Servers, Systems, Methods and Computer Program Products*,

improve the security of e-payments, credit card infrastructures and members¹³ remain very vulnerable to a number of computer attacks, such as Distributed Denial of Service (“DDoS”) attacks and frauds. In a 2014 payment fraud survey, credit cards were considered by 73% of non-financial firms as being one of the payment methods most susceptible to fraud endeavors, a very significant increase from the previous years, the majority of these firms attributing the fraud losses increase to credit card payments.¹⁴

The growing phenomenon of credit card fraud is a major concern for stakeholders, for a number of reasons. Credit card fraud losses can be up to 10 cents per \$100 of the transaction value.¹⁵ In the U.S., in 2012, the number of fraudulent transactions by credit card was 13.7 million, with a total value of \$2.3 billion.¹⁶ A high level of credit card fraud can negatively impact consumers trust. Consumer trust is an important social capital indicator,¹⁷ a determining factor of economic growth,¹⁸ and a major factor in purchase intentions.¹⁹ This can damage the reputation of the brands, and

U.S. Patent No. 20,150,026,066 (22 Jan. 2015); Paul Myers, *Electronic payment systems and methods involving a mobile device*, U.S. Patent No. 20,150,006,388 (1 Jan. 2015); L. E. E. Choong-Min et al., *Method and apparatus for electronic payment in electronic device*, U.S. Patent Application 14/202,413 (2014); Anderson, Roy L., Jacob Y. Wong & Larry Routhenstein, *Electronic card*, U.S. Patent No. 8,690,055 (8 Apr. 2014); Ralf Ohlhausen, *Electronic payment system*, U.S. Patent No. 20,140,365,371 (11 Dec. 2014); Michael Suitner, *Method and device for carrying out cashless payment*, U.S. Patent No. 20,140,344,157 (20 Nov. 2014).

¹³ See 18 U.S.C. 1029(e)(7) (defining credit card system member as “a financial institution or other entity that is a member of a credit card system, including an entity, whether affiliated with or identical to the credit card issuer, that is the sole member of a credit card system”).

¹⁴ See 2014 *Payments Fraud Survey Summary of Regional Results*, FEDERAL RESERVE BANK OF MINNEAPOLIS 14, 22 (2014) <https://www.minneapolisfed.org/about/what-we-do/payments-information> (displaying which payment methods remained most susceptible to fraud).

¹⁵ See Julia S. Cheney et al., *The Efficiency and Integrity of Payment Card Systems: Industry Views on the Risks Posed by Data Breaches*, FEDERAL RESERVE BANK OF CHICAGO 9 (2012) <https://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2012/D-2012-Efficiency-and-Integrity-of-Payment-Card-Systems.pdf> (calculating the cost allocated to consumers to compensate for credit card fraud).

¹⁶ See Federal Reserve System, *supra* note 1, at 32 (detailing prevalence of fraudulent credit card transaction in U.S. economy).

¹⁷ See Luigi Guiso, Paola Sapienza & Luigi Zingales, *The Role of Social Capital in Financial Development*, 94 AMERICAN ECONOMIC REVIEW 526, 544-45 (2004) (depicting how fraud can negatively impact economy); see also CHRISTIAAN GROOTAERT, ET AL., *Understanding and Measuring Social Capital: A Multidisciplinary Tool for Practitioners* 43-44 (Christiaan Grootaert & Thierry Van Bastelaer, eds., The World Bank 2002) (explaining indicators of social capital).

¹⁸ See Kirk Hamilton, *Where is the Wealth of Nations?: Measuring Capital for the 21st Century*, WORLD BANK 92-93 (2006), <http://siteresources.worldbank.org/INTEEI/214578-1110886258964/20748034/All.pdf> (highlighting importance of consumer trust to an efficient economy).

¹⁹ See Chao-Min Chiu et al., *Understanding customers' repeat purchase intentions in B2C e-*

reduce the use or acceptance of credit cards.²⁰

Particularly worrisome is the online victimization rate,²¹ as electronic commerce represents an increasing percentage of the overall trade,²² with credit card as an important method of payment.²³ Moreover, in certain massive breaches²⁴ where credit card data was compromised, customers sued companies.²⁵

Financial gain is by far the most powerful motivation behind credit card frauds, however, these offenses can also be encountered as hacktivism, for instance the case where criminals used the credit card of a judge to

commerce: the roles of utilitarian value, hedonic value and perceived risk, 24 INFORMATION SYSTEMS JOURNAL 85 (2014); Yulin Fang, *Trust, Satisfaction, and Online Repurchase Intention: The Moderating Role of Perceived Effectiveness of E-commerce Institutional Mechanisms*, 38 MIS QUARTERLY 407 (2014); Tao Zhou, *An empirical examination of continuance intention of mobile payment services*, 54 DECISION SUPPORT SYSTEMS 1085 (2013).

²⁰ See Form 10-K, VISA INC., *supra* note 11 at 24 (describing how widespread credit card reduces a consumers willingness to utilize credit cards).

²¹ See *Comprehensive Study on Cybercrime*, UNITED NATIONS OFFICE ON DRUGS AND CRIME 25 (2013), http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (displaying cyber-crime victimization statistics); *2014 LexisNexis True Cost of Fraud Survey: Post-Recession Revenue Growth Hampered by Fraud as all Merchants Face Higher Costs*, LEXISNEXIS 13 (2014), <http://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (illustrating the victimization rate of credit card fraud). The victimization rate is particularly worrisome because consumers increasingly turn to credit cards to complete many transactions.

²² See *Quarterly Retail E-Commerce Sales 3rd Quarter 2014*, U.S. DEPARTMENT OF COMMERCE 2 (2014), <http://www2.census.gov/retail/releases/historical/ecom/14q3.pdf> (displaying increased usage of electronic payment systems).

²³ Jip de Lange, Alessandro Longoni & Adriana Screpnic, *Online payments 2012: Moving beyond the web* 13 (2012), www.ecommerce-europe.eu/stream/report-online-payments-2012 (reviewing global trends in payment systems); *Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*, CIVIC CONSULTING 18-21 (2011), http://ec.europa.eu/consumers/archive/consumer_research/market_studies/docs/study_ecommerce_goods_en.pdf (detailing consumer spending habits).

²⁴ See Richard J. Sullivan, *Controlling security risk and fraud in payment systems*, 3 FEDERAL RESERVE BANK OF KANSAS CITY ECONOMIC REVIEW 47 (2014); Brian Krebs, *Hacker Ring Stole 160 Million Credit Cards*, KREBSONSECURITY (July 25, 2013), available at <http://krebsonsecurity.com/2013/07/hacker-ring-stole-160-million-credit-cards/> (last visited Nov. 10, 2014); Tech News, *Big Data Breach: 360 Million Newly Stolen Credentials For Sale*, NBCNEWS (Feb. 25, 2014), available at <http://www.nbcnews.com/#/tech/tech-news/big-data-breach-360-million-newly-stolen-credentials-sale-n38741> (last visited Nov. 10, 2014).

²⁵ See Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74 (2014); *Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735 (N.D. Ill. Sept. 16, 2014); *Federal Trade Commission v. Wyndham Worldwide Corporation*, No. 13-1887 (ES) (D.N.Y. Apr. 7, 2014); Consolidated Class Action Complaint, In re: Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (D. Minn. Aug. 1, 2014), <http://blogs.reuters.com/alison-frankel/files/2014/09/targetdatabreach-bankcomplaint.pdf> (last visited Nov. 12, 2014); In re TJX Companies Retail Sec. Breach Litigation, 564 F.3d 489 (1st Cir. 2009).

purchase sex toys for him,²⁶ or OpRobinHood, where members of the Anonymous and TeaMp0isoN hacking groups carried out unauthorized credit card transactions for the benefit of the poor.²⁷ Credit card frauds can take highly elaborated forms, executed by globally active organized crime groups (“OCGs”),²⁸ affecting a very large number of victims.²⁹ Even more disquieting, there are cases where the criminal activity involved money laundering³⁰ and reports stating that credit card frauds represent a funding source for terrorists.³¹

While there are many publications on various aspects of credit card fraud,³² existing studies do not present comprehensive examinations,

²⁶ See Lisa Vaas, *TeamBerserk hackers use US judge's credit card to buy sex toys for him* (2013), available at <https://nakedsecurity.sophos.com/2013/12/12/teamberserk-hackers-use-us-judges-credit-card-to-buy-sex-toys-for-him/>, (last visited Apr. 7, 2015).

²⁷ See Steve Ragan, *Anonymous and TeaMp0isoN Target Banks to Help Those “Cheated” by the System*, SECURITYWEEK (2011), available at <http://www.securityweek.com/anonymous-and-teamp0ison-target-banks-help-those-cheated-system> (last visited Nov. 10, 2014).

²⁸ See *United States v. Guvercin*, 10 Cr. 1206-01 (RWS) (S.D.N.Y. Feb. 7, 2013) (covering multiple criminal acts in Canada, Dominican Republic, Dubai, Italy, Norway, Nepal, Pakistan, the United States, etc.); *United States v. Tragas*, 727 F.3d 610 (6th Cir. 2013) (reviewing a defendant as a middleman between suppliers of stolen card data from abroad and “end-users” of such information); Europol, *Major international network of payment card fraudsters dismantled* (2011); FBI, *High-tech heist - 2,100 ATMs worldwide hit at once* (2009), available at http://www.fbi.gov/news/stories/2009/november/atm_111609 (last visited Oct. 11, 2014), discussing criminal activity that took place in 280 cities, on 3 continents; FBI, *‘Dark Market’ takedown* (2008), available at http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (last visited Oct. 11, 2014), discussing global credit card criminality.

²⁹ See *United States v. Watt*, 707 F. Supp. 2d 149 (D. Mass. 2010), the “largest conspiracy to commit identity theft in American history”; *United States v. Ortiz*, No. 13-13004, Non-Argument Calendar (11th Cir. Mar. 21, 2014), the conspiracy spanned at least 40 U.S. states; *United States v. Washington*, 714 F.3d 1358 (11th Cir. 2013), with 70 banks and financial institutions as victims.

³⁰ See cases brought in violation of 18 U.S.C. §§ 1029 and 1956 or 1957: *United States v. Guvercin*, 10 Cr. 1206-01 (RWS) (S.D.N.Y. Feb. 7, 2013), perpetrators laundered internationally the proceeds of the fraud, through hawala banks and money exchangers, in violation of 18 U.S.C. § 1956(a)(2)(B)(i); *United States v. Donahue*, No. 3: 08cr221 (M.D. Pa. June 23, 2014); *United States v. Greenberg*, No. 12-CR-301 (ADS)(ARL) (E.D.N.Y. Oct. 14, 2014); *United States v. Rojas*, No. CR14-4015-MWB (N.D. Iowa Sept. 8, 2014); *United States v. Vega*, No. 7-CR-707 (ARR) (E.D.N.Y. May 29, 2012); *United States v. Dagostini*, No. 04-CR-146 (E.D. Wis. Dec. 1, 2005). See also Europol, *Internet facilitated organised crime* (2014), available at <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta> (last visited Nov. 5, 2014) and *Stolen credit cards laundered through new criminal software “Voxis Platform”* (2014), available at <https://www.intelcrawler.com/news-23> (last visited Nov. 5, 2014).

³¹ See Louise I. Shelley et al., *Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism* (2005) at 36; G. Cliff, C. Desilets, “White collar crime: what it is and where it’s going”, 28 NOTRE DAME J.L. ETHICS & PUB. POL’Y 481 (2014); United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes* (2012) at 38; L.I. Shelley et al., *Methods and motives: exploring links between transnational organized crime & international terrorism* (2005) at 78.

³² See Dahli Gray & Jessica Ladig, *The Implementation of EMV Chip Card Technology to*

involving the study of a significant number of real cases, in order to expose and discuss the important characteristics of these crimes. This article aims to address that gap and presents findings based on the study of well over two hundred cases brought to U.S. courts in violation of 18 U.S.C. § 1029(a)(1)-(5), publications of central banks and international organizations, press releases from law enforcement organizations, such as the Federal Bureau of Investigation (“FBI”) and Europol, and information security reports. This comprehensive approach allowed the exploration of phenomenon’s multiple facets and revealed many issues that need to be considered by the stakeholders. The article, divided into four parts, discusses the legal elements, the most important perpetration aspects, and the most relevant sentencing enhancements for these offenses, and, in the conclusion, proposes several legislative, judicial and system security improvements.

II. LEGAL ELEMENTS

Credit card frauds may be prosecuted under various federal laws, such as access devices fraud (18 U.S.C. § 1029), bank fraud (18 U.S.C. § 1344), federal mail fraud (18 U.S.C. § 1341), or the wire fraud statutes (18 U.S.C. § 1343).³³ Section 1029 was enacted under the Credit Card Fraud Act (1984), part of the Comprehensive Crime Control Act of 1984,³⁴ expanded upon the provisions at 15 U.S.C. § 1644 (Truth in Lending Act) and at 15 U.S.C. § 1693n (Electronic Funds Transfer Act).³⁵ For the scope of this study, the first five subsections of 18 U.S.C. § 1029 (a) are of

Improve Cyber Security Accelerates in the U.S. Following Target Corporation's Data Breach, 6 INTERNATIONAL JOURNAL OF BUSINESS ADMINISTRATION 60 (2015); A. Dal Pozzolo et al., *Learned lessons in credit card fraud detection from a practitioner perspective*, 41 EXPERT SYSTEMS WITH APPLICATIONS 4915 (2014); Eric T. Glynn, *The Credit Industry and Identity Theft: How to End an Enabling Relationship*, BUFF. L. REV., vol. 61, 2013, pp. 215-251; Mark MacCarthy, *Information Security Policy in the U.S. Retail Payments Industry*, 2011 STAN. TECH. L. REV. 1 (2011); Lydia Segal, Benjamin Ngugi & Jafar Mana, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743 (2011); Richard A. Epstein & Thomas P. Brown, *Cybersecurity in the Payment Card Industry*, 75 U. CHI. L. REV. 203 (2008).

³³ See Alexa Briscoe, *Mail and Wire Fraud*, 50 AM. CRIM. L. REV. 1245 (2013); *United States v. Kismat*, n. 13-4779 (3d Cir. June 20, 2014); *United States v. Guvercin*, 10 Cr. 1206-01 (RWS) (S.D.N.Y. Feb. 7, 2013); *United States v. Ohanaka*, n. H-09-273-5 (S.D. Tex. Mar. 1, 2013); *United States v. Otuya*, 720 F.3d 183 (4th Cir. 2013); *United States v. Adetiloye*, 716 F.3d 1030 (8th Cir. 2013); *United States v. Magassouba*, 619 F.3d 202 (2d Cir. 2010); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *United States v. Mobley*, 618 F.3d 539 (6th Cir. 2010).

³⁴ Pub. L. No. 98-473, 98 Stat. 2183-4 (1984).

³⁵ Charles Doyle, *Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws*, CONGRESSIONAL RESEARCH SERVICE (2010) at 51.

interest: (1) the knowing, with intent to defraud, production,³⁶ use,³⁷ or traffic³⁸ in of one or more counterfeit access devices;³⁹ (2) the knowing, with intent to defraud, traffic in or use of one or more unauthorized access devices⁴⁰ during any one-year period, by such conduct obtains anything of value, aggregating to at least \$1,000 during the period; (3) the knowing, with intent to defraud, possession of fifteen or more devices, which are counterfeit or unauthorized; (4) the knowing, with intent to defraud, production, traffic in, control, custody or possession of device-making equipment;⁴¹ and (5) the knowing, with intent to defraud, effectuation of transactions with access devices issued to another person, to receive payment or any other thing of value, aggregating to at least \$1,000 during any 1-year period.⁴²

A. Intent to Defraud

All subsections require the “intent to defraud” as an element of the offense. The “intent to defraud” means that the perpetrator “is conscious of the natural consequences of his action (i.e., that it is likely that someone will be defrauded) and intends that those consequences should occur (i.e., he intends that someone should be defrauded)”.⁴³ The intent to defraud

³⁶ See 18 U.S.C. § 1029(e)(4) (defining produce as including “design, alter, authenticate, duplicate, or assemble”).

³⁷ See 15 U.S.C. § 1602(p) (defining unauthorized use as “use of a credit card by a person other than the cardholder who does not have actual, implied, or apparent authority for such use and from which the cardholder receives no benefit”).

³⁸ See 18 U.S.C. § 1029(e)(5) (defining traffic as meaning to “transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of”).

³⁹ See 18 U.S.C. § 1029(e)(1) (defining access device as “any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)”). “Counterfeit access devices” is defined at 18 U.S.C. § 1029(e)(2) as “any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device”.

⁴⁰ See 18 U.S.C. § 1029(e)(3) (defining unauthorized access devices as “any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud”).

⁴¹ See 18 U.S.C. § 1029(e)(6) (defining device-making equipment as “any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device”).

⁴² See *Criminal Resource Manual*, available at http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01027.htm (last visited Nov. 3, 2014). Subsection (a)(5) became effective September 13, 1994, as part of the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 250007, 108 Stat. 1976.

⁴³ See Charles Doyle, *supra* note 35, at 48.

involves defendant's state of mind,⁴⁴ and may be demonstrated by direct or circumstantial evidence.⁴⁵

To prove the intent to defraud, courts may consider evidence concerning prior similar acts by the defendants. In *Caputo*, for instance, Secret Service agents retrieved, from a garbage can, a bag placed there by the defendants, containing imprints of about 60 credit cards on restaurant checks.⁴⁶ The fingerprints of one defendant were discovered on three checks, even though he was not a restaurant employee, nor otherwise entitled to possess those checks; the defendants, however, negated the possession of the numbers with intent to defraud.⁴⁷ The court considered that the previous involvement of the defendants with fraudulent schemes was probative of their fraudulent intent in possessing the unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3).⁴⁸

The use of a re-issued credit card after the cardholder's demise offers an interesting examination of the defendant's intent. In *Bayard*, for illustration, the defendant, who lived in the house of a senior woman, helping her with various tasks, gained possession and used a card re-issued to the woman after her passing.⁴⁹ The defendant, convicted in violation of 18 U.S.C. § 1029(a)(2), claimed that he was specifically authorized to use the woman's cards, for the benefit of both of them, and that the transactions in the case should be considered advances on the money the woman bequeathed him.⁵⁰ However, the fact that the defendant applied for a credit card in the woman's name when she was incapacitated, and also used the card after the woman's passing, was considered relevant and probative in establishing the defendant's fraudulent intent.⁵¹

Lack of intent to defraud may be claimed when the device in the defendant's possession isn't fully functional. In *Kaba*,⁵² for example, the defendant, convicted under 18 U.S.C. § 1029(a)(3), argued that the prosecution failed to prove that "fifteen or more devices" in his possession were operational. The court, however, concluded that defendant's

⁴⁴ See Ellen S. Podgor, *Criminal Fraud*, 48 AM. U. L. REV. 729 (1999); Albert J. Harno, *Intent in Criminal Conspiracy*, 89 U. PA. L. REV. 625 (1941); Henry T. Terry, *Intent to Defraud*, 25 YALE L. J. 87 (1915).

⁴⁵ *United States v. Dodson*, No. 08-5838-cr (2d Cir. Dec. 17, 2009); *United States v. Samaria*, 239 F.3d 228 (2d Cir. 2001).

⁴⁶ *United States v. Caputo*, 808 F.2d 963, 968 (2d Cir. 1987).

⁴⁷ *Id.* at 965.

⁴⁸ *Id.* at 968-9.

⁴⁹ *United States v. Bayard*, 642 F.3d 59, 61 (1st Cir. 2011).

⁵⁰ *Id.* at 62.

⁵¹ *Id.*

⁵² *United States v. Kaba*, No. 13-10926 (11th Cir. June 16, 2014).

possession of cards encoded with numbers different than the numbers embossed, a card encoder, blank credit cards, and credit card numbers stored on his computers, sufficed to determine that the defendant acted with the intent to defraud. In the same case, regarding his conviction under 18 U.S.C. § 1029(a)(4), the defendant argued that the intent to defraud should not be deduced from “the mere possession of a non-functional” encoder. The court, however, rejected the argument, pointing out that the statute does not require the card encoder to be functional, and, also considering that software for the card encoder was found on the defendant’s computers, held the presence of the intent to defraud.⁵³

Fraudulent intent may be implied by evidence showing the defendant’s attempt to disguise the illicit activity.⁵⁴ In *Presley*,⁵⁵ for illustration, the defendant applied for a credit card in the name of her employer, without authorization. While the defense argued that Presley was “acting with actual, implied and/or apparent authority” from her boss, and not with fraudulent intent, the fact that the card was mailed to her home address, supported the intent to defraud element.⁵⁶

In *Nixon*, by contrast, the defendant, accountant for a law firm, was found in violation of 18 U.S.C. § 1029(a)(2), for using her firm’s credit card for unauthorized personal charges.⁵⁷ The court of appeals, however, emphasized that it is essential that “the intent to defraud be present both when the ‘access device’ is obtained and when it is later used,” whereas the facts in the case show that the defendant was authorized to obtain the credit card for her firm’s use.⁵⁸ As the defendant’s fraudulent intent at the time the card was obtained could not be proven. Unlike the subsequent unauthorized use of the card, the prosecution admitted that the judgment should be reversed.⁵⁹

In *Jacobowitz*, the court examined the nature of intent in the use of legitimate credit cards.⁶⁰ The defendant gave his credit cards to a friend, with the understanding that the cards will be charged, then reported as lost.⁶¹ When contacted by a card issuer in connection with the account transactions, the defendant declined responsibility for the charges.⁶² The

⁵³ *Id.*

⁵⁴ *See* United States v. Prows, 118 F.3d 686 (10th Cir. 1997).

⁵⁵ United States v. Presley, No. 5: 12cr2-DCB-FKB (S.D. Miss. Aug. 31, 2012).

⁵⁶ *Id.*

⁵⁷ United States v. Nixon, 694 F.3d 623, 625 (6th Cir. 2012).

⁵⁸ *Id.* at 638.

⁵⁹ *Id.*

⁶⁰ United States v. Jacobowitz, 877 F.2d 162 (2d Cir. 1989).

⁶¹ *Id.* at 163.

⁶² *Id.* at 164.

court reasoned that the use of a credit card by a third party, with the intent to defraud the card issuer, with cardholder's consent, even when the card was obtained without intent to defraud, violates 18 U.S.C. § 1029(a)(2).⁶³

In order to violate the statute, it is sufficient for the defendants to "receive" the required amount, without the need to "keep" or "retain" the payment.⁶⁴ Thus, it is legally irrelevant if the results of frauds are intended to be temporary or permanent.⁶⁵ In *Klopf*, for example, the defendant was convicted by the district court for the use of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(2).⁶⁶ On appeal, the defendant argued that the requisite intent to defraud cannot be proven, since all he did was to use "the creditworthiness of unsuspecting individuals to open corporate accounts in order to utilize credit cards because he was unable to apply for credit cards under his own name because of his fugitive status",⁶⁷ making regular payments on the credit accounts.⁶⁸ However, the court reasoned that defendant's undisputed intent was to deceive the card issuers into thinking that he was the person named on the cards he obtained.⁶⁹

B. Access Device

In a number of cases, defendants disputed that they possessed "access devices." In *Heath*,⁷⁰ for instance, the defendant possessed over 200 valid credit card numbers, however, he argued that card numbers by "themselves do not constitute 'access devices' within the meaning of 18 U.S.C. § 1029," as the numbers do not suffice in creating counterfeit credit cards. The court, however, noted that the defendant's actions, such as the renting of hotel rooms by using credit card numbers, ascertained that it is not necessary to create an actual credit card, in order "to obtain money, goods, services, or any other thing of value."⁷¹

In *Jones*, the defendant argued that "fictitious," expired card numbers, and cards without security codes cannot be considered "access devices" under this statute.⁷² Expired card numbers, however, are explicitly included in the definition of "unauthorized access devices" at 18 U.S.C. §

⁶³ *Id.* at 167.

⁶⁴ *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

⁶⁵ *United States v. Olson*, 925 F.2d 1170, 1175 (9th Cir. 1991).

⁶⁶ *United States v. Klopf*, 423 F.3d 1228 (11th Cir. 2005).

⁶⁷ *Id.* at 1239.

⁶⁸ *Id.* at 1240.

⁶⁹ *Id.*

⁷⁰ *United States v. Heath*, No. 10-7087, 424 F. App'x 730 (10th Cir. May 25, 2011).

⁷¹ *Id.*

⁷² *United States v. Jones*, 557 F. Supp. 2d 630, 638 (E.D. Pa. 2008).

1029(e)(3). Numbers generated randomly, on the other hand, wrongly named “fictitious” numbers by the defendant, if attached to credit cards, and not in themselves, such as numbers written on paper, in a manner that would convince a potential victim that the card is real, can also be considered counterfeit access devices.⁷³ The court further held that cards that have no data recorded on the magnetic strip should also be considered “access devices”, since “access device” is also one which can be used “in conjunction with another access device,” and such cards could be used as secondary forms of identification, for instance when applying for a store card.⁷⁴ The court also reasoned that the cards that do not have the security code are well within the definition of “access device,” because the cards could be used fraudulently even without the security codes required for online transactions.⁷⁵

An even more interesting contention as to what constitutes “access device” can be found in connection with “valid, but yet unassigned” credit card numbers. In *Taylor*, the defendant hacked into the American Express system, tried sets of combinations until he obtained valid numbers, and, in conjunction with fictitious names, was able to effectuate transactions.⁷⁶ While the defendant argued that he did not have an unauthorized access device “because no account existed, thus, he could not access an account,” the court reasoned “the language of section 1029, ‘account number, or other means of account access,’ expressly covers the transactions made by the defendant”.⁷⁷

To invalidate charges, the defendants also claim the “access devices” are not capable of being used. In *Onyesoh*, for exemplification, the defendant was convicted under 18 U.S.C. § 1029(a)(3), however, the court of appeals vacated the sentence, reasoning that, for unauthorized access devices not evidently usable, such as expired credit card numbers, if the fact is not acknowledged by the defendant, the evidence of usability is required.⁷⁸ On remand, based on expert testimony, according to which the perpetrators could use expired card numbers to get a duplicate card mailed to them, and even for certain online transactions, the court concluded that all the expired credit card numbers in the case were “usable” under the “access device” purview.⁷⁹

⁷³ *Id.* at 639.

⁷⁴ *Id.*

⁷⁵ *Id.* at 640.

⁷⁶ *United States v. Taylor*, 945 F.2d 1050, 1051 (8th Cir.1991).

⁷⁷ *ibidem*.

⁷⁸ *United States v. Onyesoh*, 674 F.3d 1157, 1160 (9th Cir. 2012).

⁷⁹ *United States v. Onyesoh*, No. 12-50363, 549 F. App'x 700, 701-02 (9th Cir. Dec. 13,

In *Miralles*,⁸⁰ on the other hand, the defendant was found in violation of 18 U.S.C. § 1029(a)(3), for having downloaded from the Internet 26,418 stolen credit card numbers. On appeal, the defendant argued that, according to 18 U.S.C. § 1029(e)(1), the numbers, in order to qualify as “unauthorized access devices,” need to be usable (i.e., operational, to obtain anything of value), whereas certain numbers in his possession were connected with accounts closed before he obtained those numbers. The court, however, reasoned that the defendant is not entitled to relief, as the error did not affect his substantial rights.⁸¹

Since 18 U.S.C. § 1029(a)(3) requires “fifteen or more devices,” the defendants may contend the evidence regarding the possession of the required number of access devices at any one time. In *Farkas*, as case in point, the court rejected the government’s argument that the repeated use of a particular credit card constitutes possession of “multiple unauthorized devices;” nonetheless, the defendant’s use of the same card number repeatedly was construed to render the possession of the access devices continuous.⁸² Although the defendant argued that the understanding of “possession” should be limited to the time of the unauthorized use, the court reasoned that such an incongruous interpretation is unacceptable, as it would mean that, in order to violate the statute, a defendant must use at least fifteen cards simultaneously.⁸³

To prove defendants’ knowledge that the access devices were counterfeit or unauthorized, extrinsic evidence could be admissible. In *Cloud*, an illustrative example, the defendant was charged with re-encoded gift and debit cards, in violation of 18 U.S.C. § 1029(a)(3).⁸⁴ The prosecution gave notice that it will introduce as Rule 404(b) evidence of three prior episodes, in which the defendant was charged in connection with his use of re-encoded gift cards.⁸⁵ The defendant filed a motion in limine and to strike, arguing that the material is not proper 404(b) evidence, and should be excluded under Rules 402 and 403.⁸⁶ The admissibility of evidence under the Rule 404(b) requires the following: “(1) the evidence must be relevant to some issue other than character; (2) there must be sufficient evidence for the jury to find the extrinsic act was committed; and

2013).

⁸⁰ *United States v. Miralles*, No. 12-14603, 521 F. App’x 837 (11th Cir. June 6, 2013).

⁸¹ *Id.*

⁸² *United States v. Farkas*, 935 F.2d 962, 967 (8th Cir. 1991).

⁸³ *Id.*

⁸⁴ *United States v. Cloud*, No. 13-0116-WS, 2013 WL 4658986 (S.D. Ala. Aug. 29, 2013).

⁸⁵ *Id.*

⁸⁶ *Id.*

(3) the probative value of the evidence must not be substantially outweighed by its undue prejudice.”⁸⁷ The court reasoned that the temporal proximity of the incidents cited by the prosecution was in favor of their admissibility, and that prior incidents that are very similar to a case’s circumstances, involving the defendant’s use of re-encoded access devices, as well as the difficulty of proving a mental state such as knowledge, reflects prosecution’s need for the extrinsic evidence, and denied defendant’s motion.⁸⁸

C. Conspiracy and Extraterritorial Application

If two or more persons conspire to intentionally commit access device fraud, in violation of 18 U.S.C. § 1029, each perpetrator can be held guilty of conspiracy, in violation of 18 U.S.C. § 371. To convict a defendant of conspiracy, the government must prove that the defendant “agreed with others that together they would accomplish the unlawful object of the conspiracy.”⁸⁹ Co-conspirators are responsible for the losses resulted from the reasonably foreseeable acts in the furtherance of their conspiracy.⁹⁰

The provisions of Section 1029 have extraterritorial application,⁹¹ as “a person may be charged in the place where the evil results, though he is beyond the jurisdiction when he starts the train of events of which that evil is the fruit.”⁹² In *Ivanov*, for example, the perpetrator was physically present in Russia, and used the computer there, as relevant to the case.⁹³ The defendant contended that the extraterritorial application of Section 1029 is permissible, however, the court reasoned that, since the intended and actual harmful results from defendant’s actions in Russia occurred within the United States, and the intended applicability of the statute is extraterritorial, it has jurisdiction.⁹⁴

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ *United States v. Alvarez*, 610 F.2d 1250 (5th Cir. 1980).

⁹⁰ *United States v. Rayborn*, 957 F.2d 841, 844 (11th Cir. 1992).

⁹¹ See Paul D. Empson, *Application of Criminal Law to Acts Committed outside the Jurisdiction*, 6 AM. CRIM. L. Q. 32 (1967-1968) (discussing considerations on the extraterritorial application of criminal provisions); B. J. George, *Extraterritorial Application of Penal Legislation*, 64 MICH. L. REV. 609 (1966).

⁹² *United States v. Steinberg*, 62 F.2d 77, 78 (2d Cir. 1932).

⁹³ *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001).

⁹⁴ *Id.*

III. PERPETRATION ASPECTS

Criminals effect fraudulent transaction to obtain cash advances⁹⁵ or to purchase luxury goods (like diamonds⁹⁶ or expensive watches),⁹⁷ electronics,⁹⁸ plane tickets,⁹⁹ lingerie,¹⁰⁰ etc. Credit card fraud cases can be very large-scale, with massive actual or potential losses¹⁰¹: about \$200,000,000 in *Watt*;¹⁰² \$15,000,000 in *Ortiz*;¹⁰³ \$13,449,377.04 in *Miralles*;¹⁰⁴ \$2,500,000 in *Wai-Keung*.¹⁰⁵ Credit card frauds encompass numerous forms and methods, regarding the production, use, or trafficking in of counterfeit access devices; the use or trafficking in of unauthorized access devices; and the effectuation of unauthorized transactions with access devices issued to other persons (“third-party fraud”).

A. Virtual Obtaining of Cards

Credit card numbers obtained illegally can be used for card-not-present (“CNP”) transactions (known also as “compromised numbers” fraud), such as payments made via Internet, or to counterfeit cards. There are multitudinous vectors or methods for gaining possession of card numbers, in electronic or in physical format, such as from hotel receipts¹⁰⁶ or store records. In *Sandoval*, for example, the co-conspirators lifted clientele books from luxury department stores, such as Neiman Marcus and

⁹⁵ See *United States v. Sadiq*, No. 14-1176, 579 F. App’x 485, 487 (6th Cir. Sept. 10, 2014); *United States v. Snead*, No. 09-057-ML, 2012 WL 3144024, at *1-3 (D.R.I. Aug. 1, 2012); *United States v. Klopff*, 423 F.3d 1228 (11th Cir. 2005).

⁹⁶ See *United States v. Jackson*, 346 F.3d 22 (2d Cir. 2003).

⁹⁷ See *United States v. Hung Van Tieu*, No. CR 11-00486-CJC, 2014 WL 814053 (C.D. Cal. Feb. 27, 2014); *United States v. Iyamu*, No. 09-15534, 393 F. App’x 667 (11th Cir. Aug. 20, 2010); *United States v. Wai-Keung*, 115 F.3d 874 (11th Cir. 1997).

⁹⁸ See *United States v. Taylor*, No. 11-4855, 497 Fed. App’x 320 (4th Cir. Nov. 26, 2012).

⁹⁹ See *United States v. Nuwintore*, No. 2: 07-cr-0139 WBS AC P, 2015 WL 1119627 (E.D. Cal. Mar. 11, 2015); *United States v. King*, No. 13-3197, 576 Fed. App’x 603 (7th Cir. Aug. 19, 2014).

¹⁰⁰ See *Sadiq*, 579 F. App’x at 487.

¹⁰¹ See *infra* Section 4.1 (detailing the calculation of potential losses).

¹⁰² See *United States v. Watt*, 707 F. Supp. 2d 149, 152 (D. Mass. 2010). (according to Application Note 3(F)(i) to § 2B1.1, based on the over 40 million credit cards stolen, at \$500 per card, the potential loss was over \$20 billion).

¹⁰³ *United States v. Ortiz*, No. 13-13004, 560 Fed. App’x 894 (11th Cir. Mar. 21, 2014).

¹⁰⁴ *United States v. Miralles*, No. 12-14603, 2013 WL 2451060 (11th Cir. June 6, 2013).

¹⁰⁵ *United States v. Wai-Keung*, 115 F.3d 874 (11th Cir. 1997).

¹⁰⁶ See *United States v. Clark*, Cr. No. C-11-795, 2013 WL 1767767 (S.D. Tex. Apr. 23, 2013).

Saks Fifth Avenue.¹⁰⁷ The perpetrators used credit card numbers from those books to purchase merchandise, which was either picked-up from the store, stolen once delivered, or claimed at delivery to be the actual recipient, then kept, resold, or returned for cash or merchandise credit.¹⁰⁸

Card numbers are often obtained through skimming, which involves the copying of card data, using a specialized device. This is usually accomplished when the credit card is used for a legitimate transaction, such as withdrawing cash at ATMs,¹⁰⁹ or paying for goods or services at various establishments,¹¹⁰ or captured by housekeepers from hotel guests.¹¹¹ In *Stepanian*, for illustration, the conspirators replaced the card payment terminals in several stores with altered terminals, which, when customers swiped cards, recorded the card numbers.¹¹²

Credit card numbers may also be obtained through false advertising¹¹³ or through phishing, social engineering attacks in which perpetrators try to exploit people's credulity, in a manner that mimics entities known to the victim (for instance, representatives from victim's office, the IRS, computer tech support, etc.)¹¹⁴ or victim's personal interests (like famous fashion models or actresses). Phishing can take several forms: e-mail;¹¹⁵ SMS ("SMiShing");¹¹⁶ social networks;¹¹⁷ phony web pages;¹¹⁸

¹⁰⁷ *United States v. Sandoval*, 668 F.3d 865, 867 (7th Cir. 2011).

¹⁰⁸ *Id.*

¹⁰⁹ *See United States v. Lopez*, No. 12-15703, 2013 WL 6570075 (11th Cir. Dec. 13, 2013); *United States v. Damyanov*, No. 12-4221, 2013 WL 60235 (4th Cir. Jan. 7, 2013).

¹¹⁰ *See United States v. Sanya*, No. 13-4937, 2014 WL 7210423 (4th Cir. Dec. 17, 2014); *United States v. Seignious*, No. 12-4621, 2014 WL 2937081 (4th Cir. July 1, 2014); *United States v. Cruz*, 713 F.3d 600 (11th Cir. 2013); *United States v. Smith*, No. 12-134-cr, 2013 WL 765066 (2d Cir. Mar. 1, 2013); *United States v. Diaz*, No. 10-4305, 2011 WL 2601504 (4th Cir. July 1, 2011); *United States v. Mayans*, No. 10-10460, 2010 WL 3314480 (11th Cir. Aug. 24, 2010); *United States v. Perez*, No. 10-10778, 2011 WL 2565201 (11th Cir. June 29, 2011).

¹¹¹ *See United States v. Cordero-Perez*, No. 6: 14-cr-177-Orl-22TBS, 2015 WL 403231 (M.D. Fla. Jan. 26, 2015);

¹¹² *United States v. Stepanian*, 570 F.3d 51, 53 (1st Cir. 2009).

¹¹³ *See United States v. Lawrence*, No. CR-10-11-D, 2010 WL 1875647 (W.D. Okla. May 10, 2010) (describing victims who were induced by advertisements on www.craigslist.com).

¹¹⁴ *See A. Giorgianni*, *Watch out for these impersonation scams*, CONSUMER REPORTS, August 12 (2014), available at <http://www.consumerreports.org/cro/news/2014/08/watch-out-for-these-impersonation-scams/index.htm> (last visited April 26, 2015).

¹¹⁵ *See United States v. Boceanu*, No. 07-CR-00012, 2013 WL 441072 (D. Conn. Feb. 4, 2013).

¹¹⁶ *See Elinor Mills*, *Phishing attacks via text spiked this week -- researcher*, CNET, Sept. 7, 2012, available at <http://www.cnet.com/news/phishing-attacks-via-text-spiked-this-week-researcher/> (last visited Apr. 28, 2015); *AllSouth Federal Credit Union v. Does*, No. 3: 13-cv-01035-JFA (D.S.C. June 3, 2013).

¹¹⁷ P. Wood, *Phishing on social networks: what's the value of your small biz Twitter account?*, SYMANTEC (2013), available at <http://www.symantec.com/connect/blogs/phishing-social-networks-what-s-value-your-small-biz-twitter-account>, (last visited Nov. 30, 2014).

or placement of fake applications in app-stores, which can allow man-in-the-middle (“MitM”) attacks when financial transactions occur.¹¹⁹

In a myriad of cases, credit card numbers, rightly named “the ideal illicit Internet commodity”,¹²⁰ by their nature very easily transmittable globally, were obtained via carding.¹²¹ Darknet¹²² is increasingly becoming host to “hidden services”, such as underground forums and criminal marketplaces. A number of cases show perpetrators trading card numbers through dedicated sites, such as CarderPlanet,¹²³ Lampeduza Republic,¹²⁴ Carder.su,¹²⁵ Barbarossa,¹²⁶ or other bulk Internet transactions.¹²⁷

Access to computer systems without authorization (i.e., data or system breach),¹²⁸ permitted by security flaws or insufficiencies at the

¹¹⁸ See FBI, *Operation Phish Phry* (2009), available at http://www.fbi.gov/news/stories/2009/october/phishphry_100709 (last visited June 12, 2014).

¹¹⁹ See M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, & V. Shmatikov, THE MOST DANGEROUS CODE IN THE WORLD: VALIDATING SSL CERTIFICATES IN NON-BROWSER SOFTWARE 38-49 (2012) (detailing proceedings of the 2009 ACM Conference on Computer and Communications Security).

¹²⁰ See *Internet facilitated organised crime*, EUROPOL 5 (2011), available at <file:///Users/josephmccarthy/Downloads/iocra.pdf>.

¹²¹ See Warrant for Arrest, *United States v. Hogue*, 12 MAG 1632 (S.D.N.Y. Jun 10, 2012), <http://www.justice.gov/usao/nys/pressreleases/June12/cardshop/hoguemichaelcomplaw.pdf>, (4/2/2014) (referring to carding as various criminal activities associated with stealing personal information, including credit card numbers); Aditya K. Sood, Rohit Bansal & Richard J. Enbody, *Cybercrime: Dissecting the State of Underground Enterprise*, 17 IEEE INTERNET COMPUTING 60 (2013); Kimberly Peretti, *Data Breaches: What the Underground World of Carding Reveals*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 375 (2008).

¹²² See United Nations, *Comprehensive and balanced approaches to prevent and adequately respond to new and emerging forms of transnational crime*, WORKING PAPER, 27 Jan. 2015, at 8-9, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/CONF.222/PM.1 (last visited Nov. 29, 2014); *The Internet organised crime threat assessment*, EUROPOL (2014) (describing how peer-to-peer networks within the Deep Web, operate using technologies such as TOR and I2P).

¹²³ See *Investigation leads to indictment and arrest of alleged international credit card trafficker*, U.S. SECRET SERVICE, (2010), available at http://www.secretservice.gov/press/GPA07-10_BadBIIndictment.pdf (last visited Oct. 31, 2014).

¹²⁴ See *Threats Report: Fourth Quarter 2013*, MCAFEE LABS (2013) at 8.

¹²⁵ U.S. Department of Justice, *Member of Organized Cybercrime Ring Responsible for \$50 Million in Online Identity Theft Sentenced to 115 Months in Prison*, Nov. 13 (2014), available at <http://www.justice.gov/opa/pr/member-organized-cybercrime-ring-responsible-50-million-online-identity-theft-sentenced-115> (last visited Nov. 29, 2014).

¹²⁶ See Consolidated Class Action Complaint, *supra* note 25, at 20.

¹²⁷ See *United States v. Seleznev*, No. CR11-0070RAJ (W.D. Wash. Feb. 9, 2015); *United States v. Seignious*, No. 12-4621, 2014 WL 2937081 (4th Cir. July 1, 2014); *United States v. Washington*, 714 F.3d 1358 (11th Cir. 2013).

¹²⁸ See *Global Payments breach puts 1.5 million credit card numbers at risk*, CONSUMER REPORTS, April 2 (2012), available at <http://www.consumerreports.org/cro/news/2012/04/global-payments-breach-puts-1-5-million-credit-card-numbers-at-risk/index.htm> (last visited Nov. 3, 2014) (detailing a major breach at Global Payments, a company responsible for processing credit

merchant¹²⁹ or payment processor level,¹³⁰ is another important credit card fraud vector.¹³¹ Vulnerability exploitation can commonly be encountered as the infiltration vector,¹³² such as attacks using the Transport Layer Security (“TLS”) features of OpenSSL,¹³³ or web-based attacks, such as Structured Query Language (“SQL”) injections,¹³⁴ Cross-Site Scripting (“XSS”) or Cross-Site Request Forgery (“CSRF”).¹³⁵ SQL injections, for example, are also used for exfiltration, as a means to obtain cardholder data (“CHD”).¹³⁶ Especially dangerous are the “zero-day” (“Øday”) vulnerabilities, which are not known to victims before the attack that exploits the vulnerability is carried out.¹³⁷

Once infiltrated into the victim’s system, the perpetrators can obtain personal or card data, subsequently used for illegal transactions, to apply for new credit cards, or to counterfeit cards,¹³⁸ or to install

card payments for merchants and banks, up to 1.5 million card numbers may have been stolen from its database).

¹²⁹ See Consolidated Class Action Complaint, *supra* note 15, at 11 (detailing various security measures including “firewall configuration, to ensure that “only allowed ports, services and IP addresses are communicating with your network”; “segregate the payment processing network from other non-payment processing networks”; “implement hardware-based point-to-point encryption”; “perform periodic scans on systems to identify storage of cardholder data and securely delete the data”; and “assign strong passwords to your security solution to prevent application modification”); see also Kristin Shields, Note and Comment: *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345 (2015).

¹³⁰ See *E-Shops Corp. v. US Bank Nat. Ass’n*, 678 F.3d 659, 664 (8th Cir. 2012).

¹³¹ See *In re TJX Companies Retail Sec. Breach Litigation*, 524 F. Supp. 2d 83, 86 (D. Mass. 2007) (referring to “the largest retail security breach ever”); *United States v. Ivanov*, 175 F. Supp. 2d 367 (D. Conn. 2001) (detailing when a perpetrator hacked into the computer system of a company processing credit card data and obtained the numbers stored).

¹³² See Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL’Y 283 (2006).

¹³³ See European Union Agency for Network and Information Security, *Heartbleed - a wake-up call* (2014), available at <https://www.enisa.europa.eu/publications/flash-notes/flash-note-heartbleed-a-wake-up-call> (last visited Nov. 10, 2014).

¹³⁴ See, e.g., *In re Heartland Payment Systems, Inc. Securities Litigation*, No. 09-1043 (D. N. J. 2009). SQL is a programming language, used to manage data in relational database management systems. See *id.* An SQL injection is a type of computer attack that consists in the insertion of a SQL query via the input data from the client to the application. See *id.* A successful SQL injection can lead to sensitive data from the database being exposed or allow the attacker to plant malicious code in the system penetrated. See *id.*

¹³⁵ See *2012 Global security report*, TRUSTWAVE (2012) at 32-33, available at www.secretservice.gov/Trustwave_WP_Global_Security_Report_2012.pdf (last visited Nov. 15, 2014).

¹³⁶ *Id.* at 8-9.

¹³⁷ See Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014); Michele Golabek-Goldman, *A New Strategy for Reducing the Threat of Dangerous Øday Sales to Global Security and the Economy* (2014), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2438164 (last visited Apr. 4, 2015).

¹³⁸ See *United States v. Warthen*, No. 10-10093, 2010 WL 3069635 (11th Cir. Aug. 6, 2010)

exfiltration computer contaminants¹³⁹ (“malicious software” or “malware”), for a similar end result.¹⁴⁰ A typical example is *Bonilla*, where the perpetrators installed unnamed malicious software at business centers in several hotels, which allowed them to obtain personal and financial data, subsequently used to illegally create and use credit cards.¹⁴¹ Another method employed by the attackers is input hooking, which allows the capture of user-supplied credit card numbers to computer systems by intercepting functions at the operating system level.¹⁴²

Memory scrapers are a category of malware frequently used by attackers to obtain card numbers from the random access memory (“RAM”) of the Point-of-Sale (“PoS”) systems.¹⁴³ Plentiful reports mention sophisticated malware employed in the perpetration of credit card frauds, such as Torpig,¹⁴⁴ Blackshades,¹⁴⁵ SpyEye,¹⁴⁶ Citadel,¹⁴⁷ POSCardStealer,

(describing perpetrators who used account information from the 2008 data breach at Heartland Payment Systems to make counterfeit cards); see also J. Cheney, *Heartland Payment Systems: lessons learned from a data breach* (2010), available at www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf (last visited Nov. 3, 2014) (detailing the *Warthen* breach).

¹³⁹ See CAL. PENAL CODE § 502(10) (defining computer contaminant as “any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.”).

¹⁴⁰ See Consolidated Class Action Complaint, *supra* note 25, at 15-16; *Global security report*, TRUSTWAVE (2014) at 48 (discussing the installation of a web shell to intercept credit card data submitted by users); McAfee Labs, *supra* note 124, at 7.

¹⁴¹ *United States v. Bonilla*, 579 F.3d 1233, 1238 (11th Cir. 2009).

¹⁴² See Wes Whitteker, *Point of sale (POS) systems and security*, SANS INSTITUTE (2014) at 13, available at <http://www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systems-security-35357> (last visited Nov. 12, 2014).

¹⁴³ See Whitteker, *supra* note 142, at 10-16; VISA Data Security Alert, *Preventing memory-parsing malware attacks on grocery merchants*, VISA (April 11, 2013), available at <http://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf>.

¹⁴⁴ See CSO Online, *Digital black market offers cheap botnets for hire, stolen credit card info* (2011), available at www.csoonline.com/article/657159 (last visited Nov. 2, 2014); B. Stone-Gross et al., *Your botnet is my botnet: analysis of a botnet takeover*, Proceedings of the 2009 ACM Conference on Computer and Communications Security (2009), available at <https://seclab.cs.ucsb.edu/media/uploads/papers/torpig.pdf> (last visited Nov. 4, 2014).

¹⁴⁵ See FBI, *International Blackshades malware takedown* (2014), available at <http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown> (last visited June 2, 2014).

¹⁴⁶ See U.S. Attorney’s Office, *Cyber criminal pleads guilty to developing and distributing notorious SpyEye malware* (2014), available at <http://www.fbi.gov/atlanta/press-releases/2014/cyber-criminal-pleads-guilty-to-developing-and-distributing-notorious-spyeye-malware> (last visited Nov. 3, 2014).

Alina, or ProjectHook,¹⁴⁸ and the use of various attack techniques, such as web injects, keystroke loggers or credit card grabbers. The epitome of advanced PoS malware can be considered ChewBacca, which features two mechanisms for obtaining data: a keylogger and a memory scanner, designed specifically for PoS systems, which dumps a copy of the running memory process, searches for credit card numbers and inputs the numbers found into a file.¹⁴⁹ The communications between the infected devices and the perpetrators' server are accomplished through a network of encrypted relay systems, which permit the concealment of users' identity and communications content.¹⁵⁰

The PoS attacks facilitate the obtaining of massive amounts of credit card numbers. In *Guvercin*,¹⁵¹ for illustration, the defendants installed advanced skimmers and GSM devices into PoS readers, allowing them to receive about 349,000 SMS messages, containing card numbers, subsequently disseminated worldwide, and used to manufacture counterfeited cards and obtain cash. The investigation of this case also revealed that perpetrators had a memory card containing 186,000 sets of card numbers and corresponding PINs.¹⁵²

In certain extensive cases, millions of credit card numbers are compromised.¹⁵³ The quintessential case in this regard can be considered *Gonzalez*,¹⁵⁴ where conspirators, via sniffer programs, accessed track 2 data for tens of millions of cards and PINs, subsequently encrypted, to conceal their purpose and prevent others from using the data, and stored on servers in several countries. In another high profile case, the conspirators, via interstate and international computer transmissions, obtained unauthorized access and installed sniffers on the PoS servers in several Dave & Buster's ("D&B") restaurants.¹⁵⁵ The malicious software allowed the capture of

¹⁴⁷ See 2014 Data breaches investigations report, VERIZON (2014), at 32, available at www.verizonenterprise.com/DBIR/2014/ (last visited Nov. 15, 2014).

¹⁴⁸ See McAfee Labs, *supra* note 124, at 6.

¹⁴⁹ See VISA, "Chewbacca" POS malware, March 6 (2014), available at <http://usa.visa.com/download/merchants/Alert-ChewbaccaMalware-030614.pdf> (last visited Nov. 3, 2014).

¹⁵⁰ *Id.*

¹⁵¹ *United States v. Guvercin*, 10 Cr. 1206-01 RWS, 2013 WL 466429 (S.D.N.Y. Feb. 7, 2013).

¹⁵² *Id.*

¹⁵³ See H. Dunleavy, *United States Secret Service: Protecting the Nation's Leaders and Financial Infrastructure*, in 2012 Global security report, *op. cit.*, at 20.

¹⁵⁴ *United States v. Gonzalez*, 08 CR 10223 PBS, 2009 WL 1543798 (D. Mass. May 26, 2009).

¹⁵⁵ See *United States v. Yastremskiy et al.*, 08-160(S-1)(SJF), 2008 WL 3199939 (E.D.N.Y. May 14, 2008) (superseding indictment).

track 2 data, transmitted from the compromised servers, via the system at D&B headquarters, to the data processor's computer system.¹⁵⁶

Card numbers are used in numerous cases to clone¹⁵⁷ legitimate cards, by encoding cards with perpetrator's name.¹⁵⁸ Credit cards, however, can also be counterfeit through other methods, including altering or forging. In *Meredith*,¹⁵⁹ in an elaborated approach, in violation of 18 U.S.C. § 1029(a)(1), the conspirators, in order to obtain credit cards, stole mail. Perpetrators, via an algorithm that imitated the process used by the credit card issuers to generate legitimate card numbers, created new numbers, tested via a merchant identification number, which was then used to substitute the numbers on the original cards. The cards were demagnetized, so that merchants would have to manually enter the new numbers, associated with fake identifications, and containing the conspirators' pictures.¹⁶⁰

B. Physical Obtaining of Cards

Credit cards can be physically obtained by applications under false pretenses, by theft,¹⁶¹ by presenting a false ID to the mail worker to obtain other people's mail,¹⁶² or through applications based on false identifications or identity theft,¹⁶³ in violation of 18 U.S.C. § 1028(a) or of 18 U.S.C. § 1028A(a).¹⁶⁴ In *Banks-Davis*,¹⁶⁵ for example, the defendant obtained a

¹⁵⁶ *Id.* at 4.

¹⁵⁷ See 18 U.S.C. § 1029(e)(2) (defining cloned credit card as a "copy of someone's credit card", realized by encoding card data obtained via a skimmer onto the magnetic strip of a card; a "cloned" card qualifies as "counterfeit access device"); *United States v. Keita*, 742 F.3d 184 (4th Cir. 2014).

¹⁵⁸ See *United States v. Harris*, No. 14-10016, 2015 WL 1262543 (5th Cir. Mar. 19, 2015); *United States v. Fofana*, No. 4: 11-cr-00027-1, 2014 WL 43808 (W.D. Va. Jan. 6, 2014); *United States v. Tragas*, 727 F.3d 610 (6th Cir. 2013); *United States v. Phillips*, No. 2:12-00004, 2013 WL 145983 (M.D. Tenn. Jan. 14, 2013); *United States v. Alabi*, 943 F. Supp. 2d 1201, 1213 (D.N.M. 2013); *United States v. Agyepong*, No. 09-4643, 2010 WL 2852653 (4th Cir. July 21, 2010); *United States v. Alicea*, No. 09-6213, 2010 WL 1632903 (10th Cir. Apr. 23, 2010).

¹⁵⁹ *United States v. Meredith*, No. 09-1416, 2010 WL 1225883 (10th Cir. Mar. 31, 2010).

¹⁶⁰ *Id.*

¹⁶¹ See *United States v. Becerra*, No. 13-50381 (9th Cir. Apr. 14, 2015); *United States v. King*, No. 13-3197, 2014 WL 4068575 (7th Cir. Aug. 19, 2014).

¹⁶² *Obasohan v. Attorney General*, 479 F.3d 785 (11th Cir. 2007).

¹⁶³ See LexisNexis, *Merchants struggle against an onslaught of high-cost identity fraud and online fraud* (2013); M. Richey, *Identity Theft*, DEFENDER SERVICES OFFICE TRAINING DIVISION (2010), available at <http://www.fd.org/docs/select-topics/common-offenses/identity-theft/oct-2010-update-final-x.pdf?sfvrsn=8> (last visited Nov. 15, 2014).

¹⁶⁴ See *United States v. Harris*, No. 2:10 CR 123, 2014 WL 1344277 (N.D. Ind. Apr. 4, 2014) (stating that "a person commits identity theft if they use someone else's identification while attempting to commit credit card fraud, and a person commits aggravated identity theft if they use

credit card in victim's name, claiming that she would use the card to consolidate victim's bills, however, used victim's card to charge personal expenses, in violation of 18 U.S.C. § 1029(a)(5). In *McCall*,¹⁶⁶ the perpetrators stole credit cards from the U.S. Mail, acquired personal information about the intended receivers, and used the cards to obtain goods and withdraw cash. To pass photo identification, measures used to prevent the unauthorized use of a credit card, perpetrators create fictitious driver licenses; contain their picture and the name embossed on the cards.¹⁶⁷

There are scores of cases where credit cards were obtained and used through various forms of identity theft.¹⁶⁸ In fact, according to the consumer complaints reported to, *inter alia*, the Federal Trade Commission, state law enforcement organizations and the FBI's Internet Crime Complaint Center, credit card frauds represent the second most common form of identity theft.¹⁶⁹ Identity thieves customarily collect personal identifying information, for instance dates of birth and Social Security numbers, in order to build victim's profile, based on stolen mail or credit reports, or exploiting the fact that credit card numbers do not change upon expiration, sometimes using successfully the information and obtaining new credit cards.¹⁷⁰

A major concern is represented by account "take over." This can occur when the perpetrators steal identifying information, from individuals or business entities, such as real estate agents or mortgage companies,¹⁷¹

the identification to actually commit the credit card fraud.")

¹⁶⁵ *United States v. Banks-Davis*, No. 13-4217, 2014 WL 104169 (4th Cir. Jan. 13, 2014).

¹⁶⁶ *United States v. McCall*, No. 2: 13-cr-144-MEF-TFM [wo] (M.D. Ala. Dec. 19, 2013).

¹⁶⁷ *See United States v. Johnson*, No. 3: 12-CR-00027-VLB-1, 2013 WL 6002717 (D. Conn. Nov. 12, 2013).

¹⁶⁸ *See United States v. Williams*, No. 13-2391, 2014 WL 5487799 (3d Cir. Oct. 31, 2014); *United States v. Ryan*, No. 11-20425-7, 2014 WL 2968558 (E.D. Mich. July 2, 2014); *United States v. Sadiq*, No. 14-1176, 2014 WL 4436048 (6th Cir. Sept. 10, 2014); *United States v. Marchante*, No. 11-11906, 2013 WL 1223477 (11th Cir. Mar. 26, 2013); *United States v. Calhoun*, 721 F.3d 596 (8th Cir. 2013); *United States v. Damyanov*, No. 12-4221, 2013 WL 60235 (4th Cir. Jan. 7, 2013); *United States v. Cruz*, 713 F.3d 600 (11th Cir. 2013); *United States v. Iacona*, 728 F.3d 694 (7th Cir. 2013); *United States v. Novas*, No. 11-12584, 2012 WL 762762 (11th Cir. Mar. 9, 2012); *United States v. Holstine*, No. 2: 11-cr-00096, 2012 WL 2368408 (S.D.W. Va. June 21, 2012); *United States v. Godsey*, 690 F.3d 906 (8th Cir. 2012); *United States v. Lawrence*, No. CR-10-11-D, 2010 WL 1875641 (W.D. Okla. May 10, 2010); *United States v. Howard*, 619 F.3d 723 (7th Cir. 2010); *United States v. White*, 620 F.3d 401 (4th Cir. 2010); *United States v. Smaw*, 22 F.3d 330 (D.C. Cir. 1994).

¹⁶⁹ *See Federal Trade Commission, Consumer Sentinel Network Data Book*, 3 (February 2014) available at <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf>.

¹⁷⁰ *See United States v. Onyesoh*, No. 12-50363, 2013 WL 6512048 (9th Cir. Dec. 13, 2013).

¹⁷¹ *See United States v. Snead*, No. 09-057-ML, 2012 WL 3144024 (D.R.I. Aug. 1, 2012).

then add their or other names onto the credit card account, pretend to the financial institutions to be the legitimate account holder, or act in collusion with an insider, subsequently causing illegal activity on the account, in violation of 18 U.S.C. § 1029(a)(2).¹⁷² In *Auguste*,¹⁷³ for instance, an American Express employee supplied the account number of a customer to the defendant, who added herself onto the account as a secondary cardholder, then modified the account's mailing address, so that she would obtain a credit card in her name.

Identity theft involves a plethora of manners and means of perpetration, as follows. In *Ward*,¹⁷⁴ in an international fraud scheme, the conspirators acquired victims' personal information, used via phone calls for impersonation, and obtained and used replacement credit cards. In *Doss*,¹⁷⁵ the perpetrator created fake identification documents and sold the documents to individuals who obtained credit cards based on those materials. In *Madera*,¹⁷⁶ the offender, using valid dates of birth and social security numbers, applied online for and obtained credit cards in the names of different individuals. In *Jenkins-Watts*,¹⁷⁷ perpetrators applied for instant credit based on credit reports acquired from legitimate businesses. In *Maurello*,¹⁷⁸ the defendant, based on biographical information gathered from obituaries, acquired birth certificates and other personal information from public records, then applied and obtained credit cards under assumed names.

In *Abiodun*,¹⁷⁹ the conspirators illegally acquired and made use of credit reports and bank documents, some containing the name and photo of the fraud victim, to obtain credit cards. In *Ahmid*,¹⁸⁰ perpetrators exploited "files"¹⁸¹ of people that departed or that were deported from the U.S., in association with members of a fraud ring. In *Morris*, the defendant opened

¹⁷² See *United States v. Bass*, No. 14-1387 (6th Cir. Apr. 15, 2015); *United States v. Harris*, Cause No. 2: 10 CR 123, 2014 WL 1344277 (N.D. Ind. Apr. 4, 2014); *United States v. Bradshaw*, No. 10-15780, 2011 WL 3911094 (11th Cir. Sept. 7, 2011); *United States v. Oladokun*, 760 F. Supp. 2d 57, 62 (D.C. 2011).

¹⁷³ *United States v. Auguste*, 392 F.3d 1266 (11th Cir. 2004).

¹⁷⁴ *United States v. Ward*, No. 12-50536, 2014 WL 1317155 (9th Cir. Apr. 3, 2014).

¹⁷⁵ *United States v. Doss*, No. 13-1001, 2013 WL 6698046 (7th Cir. Dec. 20, 2013).

¹⁷⁶ *United States v. Madera*, No. 13 Cr. 415 (RWS), 2013 WL 6284420 (S.D.N.Y. Dec. 4, 2013).

¹⁷⁷ *United States v. Jenkins-Watts*, 574 F.3d 950, 956 (8th Cir. 2009).

¹⁷⁸ *United States v. Maurello*, 76 F.3d 1304 (3d Cir. 1996).

¹⁷⁹ *United States v. Abiodun*, 536 F.3d 162 (2d Cir. 2008).

¹⁸⁰ *United States v. Ahmid*, No. 10 Cr. 195-03 (RWS), 2011 WL 5119577 (S.D.N.Y. Oct. 28, 2011).

¹⁸¹ See *id.* at *3. A "file" usually contains person's name, mailing address, social security number, birth date, mother's maiden name and phone number.

credit accounts by using the information obtained from the women she was fostering.¹⁸² In *Cantey*,¹⁸³ perpetrators opened credit accounts using the personal information of defunct or elderly victims.

In *Akinkoye*,¹⁸⁴ the defendant, a real estate agent, submitted applications and obtained credit cards in the name of his clients. The cards were delivered to victim's homes or mailboxes, taken from there by the defendant, who used the keys provided by the clients.¹⁸⁵ As a number of his clients were women, he recruited Afolabi, who provided her photo for the identification associated with the cards.¹⁸⁶

C. Abuse of a Position of Trust

A considerable number of cases regarding the effectuation of fraudulent transactions involve abuse of a position of trust.¹⁸⁷ As observed in *Craddock*, "one has been placed in a position of trust when, by virtue of the authority conferred by the employer and the lack of controls imposed on that authority, he is able to commit an offense that is not readily discoverable."¹⁸⁸ Such cases are of major concern as such positions significantly facilitate the criminal activity and often offer the means and knowledge to conceal the offense, or to make it go undiscovered for a very long time.

In *Hatton*,¹⁸⁹ for example, the defendant used her employer's and her mother's credit cards for unauthorized personal charges, in violation of 18 U.S.C. § 1029(a)(5). In *Lazarus*,¹⁹⁰ the perpetrator, employed by a travel agency, used the card numbers of old customers to book vacations for her new customers, who paid via PayPal, money misappropriated subsequently by the defendant. In *Chowdhury*,¹⁹¹ the perpetrator, a store employee, obtained, without authorization, copies of card numbers, afterwards used to

¹⁸² *United States v. Morris*, 350 F.3d 32 (2d Cir. 2003).

¹⁸³ *United States v. Cantey*, No. 11-2835, 2012 WL 2478343 (3d Cir. June 29, 2012).

¹⁸⁴ *United States v. Akinkoye*, 185 F.3d 192 (4th Cir. 1999).

¹⁸⁵ *Id.* at 196.

¹⁸⁶ *Id.* at 197.

¹⁸⁷ See Matthew S. Rozen, *Abandoning the Victim Requirement: Clarifying the Position of Trust Enhancement in Federal Sentencing*, 78 U. CHI. L. REV. 1543 (2011) (discussing the "position of trust" and the abuse of such a position); see also *United States v. Ollison*, 555 F.3d 152 (5th Cir. 2009).

¹⁸⁸ *United States v. Craddock*, 993 F.2d 338, 342 (3d Cir. 1993).

¹⁸⁹ *United States v. Hatton*, No. 09-2216, 2010 WL 165146 (8th Cir. Jan. 19, 2010).

¹⁹⁰ *United States v. Lazarus*, No. 12-16287, 2014 WL 104212 (11th Cir. Jan. 13, 2014).

¹⁹¹ *United States v. Chowdhury*, No. 11-3003, 2011 WL 4469773 (6th Cir. Sept. 27, 2011).

fund his debit card and to order goods. In *Braggs*,¹⁹² a temporary employee, in charge of updating the names, addresses, and social security numbers of her employer's sales representatives, used that information to submit online credit card applications, opening several unauthorized accounts. In *Culbreth*,¹⁹³ the defendant, while employed as office manager, contacted without authorization the issuers of her employer's credit cards and requested to be added as authorized user on each of the cards.

Even more alarming are cases where the perpetrators own the trade, and charge customers' cards without their authorization. In *Greenberg*,¹⁹⁴ for exemplification, the defendant, owner of a clothing business, placed tens of thousands of unauthorized charges, totaling millions of dollars. In *Catching*,¹⁹⁵ the perpetrator, running a mortgage business, used victims' personal information, obtained through commercial relationships, to gain access to their credit accounts, without victims' knowledge or consent.

In some cases, the perpetrators engage in "collusive charges." These type of offenses involve colluding merchants, who fraudulently charge cards for fictitious services, subsequently paying part of the criminal proceeds (the "kkang fee")¹⁹⁶ to the providers of the fraudulent or unauthorized cards.¹⁹⁷ In *Ismoila*,¹⁹⁸ for illustration, the perpetrator, in a complex scheme, carried out fake transactions, involving fictitious merchandise, using stolen credit cards, in violation of 18 U.S.C. § 1029(a)(2).

IV. SENTENCING ENHANCEMENTS

The U.S. Sentencing Guidelines ("U.S.S.G."), represent the most important factor considered by federal courts to ensure that the sentence is "sufficient, but not greater than necessary"¹⁹⁹ despite being although non-

¹⁹² United States v. Braggs, 511 F.3d 808 (8th Cir. 2008).

¹⁹³ United States v. Culbreth, No. 10-4546, 2011 WL 2356777 (4th Cir. June 14, 2011).

¹⁹⁴ United States v. Greenberg, No. 12-CR-301 (ADS)(ARL), 2014 WL 5306553 (E.D.N.Y. Oct. 14, 2014).

¹⁹⁵ United States v. Catchings, 708 F.3d 710, 714 (6th Cir. 2013).

¹⁹⁶ See FBI, *Two plead guilty to roles in large-scale identity theft ring* (2011), available at <http://www.fbi.gov/newark/press-releases/2011/two-plead-guilty-to-roles-in-large-scale-identity-theft-ring> (last visited Nov. 30, 2014).

¹⁹⁷ See United States v. Janjua, No. 10 Cr. 195-01 (RWS), 2010 WL 4177465 (S.D.N.Y. Oct. 22, 2010).

¹⁹⁸ United States v. Ismoila, 100 F.3d 380, 386 (5th Cir. 1996).

¹⁹⁹ 18 U.S.C. § 3553(a).

mandatory recommendations.²⁰⁰ A significant number of credit card fraud cases raise interesting issues regarding the sentencing enhancements, which augment the punishment by raising the offense level. The following subsections discuss the “amount of loss,” “number of victims,” “sophisticated means,” “role in the offense” enhancements, and upward adjustments.

A. Amount of Loss

The “amount of loss” is the most common enhancement in credit card fraud cases. According to the U.S.S.G., “loss” is “effectively a proxy for evaluating culpability,”²⁰¹ and is the greater of actual loss or intended loss.²⁰² In the case of stolen or counterfeit credit cards, the loss calculation considers at least \$500 per access device.²⁰³ The loss calculation “does not have to be rigorously precise, only reasonable given the information available.”²⁰⁴ Even though the loss caused may not be the cards’ aggregate limit, the “expectation is not synonymous with intent when a criminal does not know what he may expect to obtain, but intends to take what he can.”²⁰⁵

In a number of cases, the courts calculated the intended loss as the credit limit of the cards, even where there was no evidence that the defendants actually planned to reach that limit. In *Gilmore*, the defendant argued that Application Note 3(F)(i) “only applies if a charge was made with the access device.”²⁰⁶ The court of appeals, however, pointed to a number of cases where the application of the “\$500-per-device” rule was not limited to the access devices actually used by the perpetrators, and affirmed the sentence.²⁰⁷

²⁰⁰ See *United States v. Booker*, 543 U.S. 220 (2005).

²⁰¹ See *United States v. Watt*, 707 F. Supp. 2d 149, 154 (D. Mass. 2010).

²⁰² U.S.S.G. § 2B1.1 n.3(A) (2014) (defining actual loss as “the reasonably foreseeable pecuniary harm that resulted from the offense”). “Intended loss” means the “pecuniary harm that was intended to result from the offense”, and includes “intended pecuniary harm that would have been impossible or unlikely to occur”. *Id.* “Pecuniary harm” means “harm that is monetary or that otherwise is readily measurable in money. Accordingly, pecuniary harm does not include emotional distress, harm to reputation, or other non-economic harm”, *id.*, at (i)-(iii). *Id.*

²⁰³ U.S.S.G. §2B1.1 (“In a case involving any counterfeit access device or unauthorized access device, loss includes any unauthorized charges made with the counterfeit access device or unauthorized access device and shall be not less than \$500 per access device”).

²⁰⁴ See *United States v. Ferdinand*, No. 12-14081, 2013 WL 1668238 (11th Cir. Apr. 17, 2013).

²⁰⁵ See *United States v. Kismat*, No. 13-4779, 2014 WL 2800787 (3d Cir. June 20, 2014).

²⁰⁶ *United States v. Gilmore*, No. 10-5055, 2011 WL 2623676 (6th Cir. July 6, 2011).

²⁰⁷ *Id.*

A different approach can be found in *Barry*,²⁰⁸ where the district court equated the potential loss (i.e., the aggregate credit limits, amounting in the case to \$675,170) with the intended loss, although the actual loss was just \$13,396.33, which resulted in a significant increase of defendant's offense level. The court of appeals, however, held that, while the intended loss could equal the potential loss, the former should not be determined automatically, based on the amount of the potential loss. Courts err in equating the potential loss with the intended loss without a "deep analysis."²⁰⁹ As the district court did not employ the essential "deeper analysis," the sentence was vacated and remanded for the reassessment of the amount of intended loss.²¹⁰

In *Catchings*, in the calculation of loss, the district court included losses associated with legitimate credit cards, opened and used in the name of the enterprise the defendant opened with a friend.²¹¹ However, the court of appeals reasoned that, while the defendant exploited his trusting friend, the evidence did not support the conclusion that the defendant engaged in criminal conduct in using the legitimate cards.²¹² Therefore, the case was remanded for resentencing.²¹³ In *Watt*, the defendant adapted a sniffer program, subsequently used by the co-conspirator Gonzalez to obtain credit card numbers from TJX.²¹⁴ U.S.S.G. holds the defendants accountable for "all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused"²¹⁵ and for "all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity."²¹⁶ Consequently, the defendant was held "responsible for the entire loss, as an initial matter."²¹⁷

The defendant, however, disputed the amount ascribable to him, arguing that he did not use the program and received no money for his software, and claiming that what he did was actually "for the challenge, for the thrill of besting large institutions," and "did not know about the specifics, did not access any of the information stolen, did not profit and that some of the back and forth with Gonzalez was just bravado."²¹⁸ He

²⁰⁸ United States v. Barry, No. 12-4334, 2013 WL 3970158 (3d Cir. Aug. 5, 2013).

²⁰⁹ *Id.*

²¹⁰ *Id.*

²¹¹ United States v. Catchings, 708 F.3d 710, 720 (6th Cir. 2013).

²¹² *Id.* at 721.

²¹³ *Id.* at 722.

²¹⁴ United States v. Watt, 707 F. Supp. 2d 149, 155 (D. Mass. 2010).

²¹⁵ U.S.S.G. § 1B1.3(a)(1)(A).

²¹⁶ U.S.S.G. § 1B1.3(a)(1)(B).

²¹⁷ United States v. Watt, 707 F. Supp. 2d 149, 155 (D. Mass. 2010).

²¹⁸ *Id.* at 150-156.

elaborated that his “contribution” to the fraud was “not indispensable.”²¹⁹ Undoubtedly, honest intentions prevent convictions for acts requiring *mens rea*. In this case, however, the prosecution convincingly pointed out to defendant’s participation in the extravagant parties organized by Gonzalez, and to electronic communications showing that the defendant was informed about the losses inflicted and motivated by “malicious intent to take down corporations and individuals.”²²⁰ The court, based on the provisions of 18 U.S.C. §§ 3553(a)(2)(A)-(B), considered it appropriate to impose a two year sentence and an order of restitution of \$171.5 million (i.e., the total losses inflicted to TJX).

B. Number of Victims

U.S.S.G. §2B1.1(b)(2) provides an enhancement based upon the number of victims²²¹ of the offense. This enhancement, however, can lead to double counting the pecuniary harm, which may result in sentences that overstate the seriousness of the offense.²²² Additionally, the counting of every individual linked to a misappropriated card as “victim”, even when unaffected or unaware of the fraud, may also raise excessively the offense level.²²³

As the number of victims can significantly increase the offense level,²²⁴ in several cases the defendants disputed the evidence regarding the enhancement. Representative of the type is *Washington*, where the prosecution stated that the victims were the individual cardholders, totaling over 6,000 from May 2010 to March 2011; however, the defendant joined the conspiracy only from September 2010.²²⁵ As the prosecution failed to present evidence regarding the identity of individual victims, as well as

²¹⁹ *Id.* at 150-156.

²²⁰ *Id.* at 157 (quoting Watt as saying that he had a “rush” about “ripping off somebody large and powerful”, and “[W]hat really drove me harder and further was the exciting possibility of using computers to turn the life of a particular fellow human being into a living hell”).

²²¹ See U.S.S.G. § 2B1.1. “Victim is defined in the commentary to the U.S. Sentencing Guidelines Manual (“U.S.S.G.”) as any person who sustained any part of the actual loss determined under subsection (b)(1). Person, as defined at U.S.S.G. § 2B1.1(b)(2), cmt. n. 1 (2014), includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.(internal quotation marks omitted).

²²² See Marjorie A. Meyers, *Re: Economic Offenses*, FEDERAL PUBLIC DEFENDER, July 15 (2013), at 6, available at <http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-comment/20140729/FPD.pdf> (last visited Nov. 11, 2014).

²²³ *Id.* at 7.

²²⁴ See U.S.S.G. §2B1.1(b)(2)(B)-(C) (setting forth four levels if the number of victims is 50 or more, six levels, if the number of victims is 250 or more).

²²⁵ *United States v. Washington*, 714 F.3d 1358, 1361 (11th Cir. 2013).

when card numbers were actually misused, in order to establish that the conspiracy involved 250 or more victims from September 2010 to March 2011, the court of appeal vacated the sentence and declined the government's request to prove on remand that the scheme affected 250 or more victims.²²⁶

In *Conner*, the defendant argued that, as all accounts were fully refunded for the unauthorized charges, cardholders could not be counted as victims.²²⁷ The district court, however, reasoned that “waiting until after reimbursement to measure ‘pecuniary harm’ and ‘actual loss,’ the majority’s interpretation of the victim enhancement in § 2B1.1 runs counter to the fundamental sentencing goal of tying the severity of a defendant’s sentence to the seriousness of the defendant’s crime.” A similar reasoning can be found in a number of other cases: even though losses were promptly credited by third parties, victims have suffered an initial loss.²²⁸

C. Sophisticated Means

Another common enhancement in credit card fraud cases is the “sophisticated means.” U.S.S.G. defines “sophisticated means” as an “especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense.”²²⁹ While the ability to hack into order logs in order to obtain card numbers, and to rewrite CGI scripts,²³⁰ or the use of advanced skimming technology,²³¹ clearly exceeds the knowledge of the average person, in a number of cases the application of this enhancement is less obvious.

There is no need, as reasoned in various cases, for the conduct to involve highly complex schemes, state-of-the-art technology, or exceptional skills, in order to justify the sophisticated means enhancement. For example, disguising fraudulent purchases by encoding cards with stolen numbers, so that the purchases would appear as legitimate, was considered sufficiently sophisticated to justify the enhancement.²³² This enhancement is also controversial because it allows for a double

²²⁶ *Id.* at 1362.

²²⁷ *United States v. Conner*, 537 F.3d 480, 488 (5th Cir. 2008).

²²⁸ *See United States v. Donahue*, No. 3: 08-cr-221, 2014 WL 2860884 (M.D. Pa. June 23, 2014); *United States v. Nikoghosyan*, No. 10-10073, 10-10074, 2011 69788 (11th Cir. Jan. 7, 2011); *United States v. Alicea*, No. 09-6213, 2010 WL 1632903 (10th Cir. Apr. 23, 2010).

²²⁹ U.S.S.G. § 2B1.1 cmt. n.9 (2014).

²³⁰ *See United States v. Prochner*, 417 F.3d 54 (1st Cir. 2005).

²³¹ *See United States v. Guvercin*, 10 Cr. 1206-01 (RWS), 2013 WL 466429 (S.D.N.Y. Feb. 7, 2013).

²³² *See United States v. Mendez*, No. 14-4059, 2014 WL 5786649 (4th Cir. Nov. 7, 2014).

enhancement based on the same conduct, for instance a two-level increase for “sophisticated means” if the defendant uses a card skimmer to commit the fraud, and another two-level increase for the possession or use of device-making equipment.²³³

Even in cases where no action is especially complicated or entangled, the series of criminal actions may be construed as “sophisticated means.”²³⁴ In *Lin*, for example, the investigation of defendants’ laptops revealed files containing cardholder names and card numbers, instant-messages between the defendants and individuals situated in Russia and Ukraine, regarding the acquisition of card numbers, and several wire transfers to those countries.²³⁵ The defendants used the numbers obtained fraudulently to re-encode gift cards and traveled to various locations to use the cards at self-checkout machines. The court of appeals reasoned that, even though the steps involved were not very elaborate, the district court did not clearly err in considering that, as a whole, the conspiracy involved sophisticated means.²³⁶

In *Jackson*,²³⁷ the defendant identified affluent people via Internet searches, obtained information about them, and then place phone calls to persuade the card issuers that he was the real cardholder. On appeal, the defendant argued that his acts, while fraudulent, were no more intricate than “a game of Three-Card Monte.”²³⁸ However, the court of appeals reasoned that the scheme was “sophisticated in the way all the steps were linked together so that Jackson could perceive and exploit different vulnerabilities in different systems in a coordinated way.”²³⁹

In *Calhoun*,²⁴⁰ the defendants used stolen cards to buy and resell plane tickets, in violation of 18 U.S.C. §§ 371 and 1029(a)(5). On appeal,

²³³ See Marjorie A. Meyers, *Re: Proposed Priorities for 2013-2014*, FEDERAL PUBLIC DEFENDER, May 17 (2013), at 21, available at <http://www.ussc.gov/sites/default/files/pdf/amendment-process/public-comment/20140729/FPD.pdf> (last visited Nov. 11, 2014); *United States v. Lyles*, No. 11-5774, 11-5818, 2012 WL 5907483 (6th Cir. Nov. 26, 2012); *United States v. Podio*, No. 10-40478, 2011 WL 2650931 (5th Cir. July 7, 2011);

²³⁴ See *United States v. Dancer*, No. 12-11989, 2013 WL 598336 (11th Cir. Feb. 15, 2013); *United States v. Conner*, 537 F.3d 480 (5th Cir. 2008).

²³⁵ *United States v. Lin*, No. 11-2554, 2012 WL 6176772 (6th Cir. Dec. 11, 2012).

²³⁶ *Id.*

²³⁷ *United States v. Jackson*, 346 F.3d 22 (2d Cir. 2003).

²³⁸ *Id.* at 25.

²³⁹ *Id.* The court referred to the U.S.S.G. Application, which expressly defines “sophisticated means” to include “conduct pertaining to the execution or concealment of an offense.” *Id.*

²⁴⁰ *United States v. Calhoun*, 721 F.3d 596 (8th Cir. 2013).

they argued that what they did was “a garden variety offense.”²⁴¹ The court, however, underlined that, considering the defendants’ strategies to avoid fraud detection, such as misspelling the names of cardholders and carefully choosing when to fraudulently use the cards, the application of the “sophisticated means” enhancement was not erroneous.²⁴²

D. Role in the Offense

The offense level is also increased in situations in which the defendant held an aggravating role in the offense: (a) “organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive”; (b) “manager or supervisor (but not an organizer or leader) and the criminal activity involved five or more participants or was otherwise extensive”; (c) “organizer, leader, manager, or supervisor in any criminal activity other than described in (a) or (b).”²⁴³ In ascertaining defendant’s role in the offense, courts consider “the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercised over others.”²⁴⁴ The “organizer” or “leader” exercises a “significant degree of control and decision making authority over the criminal activity,” while a “manager” or “supervisor” only exercises a certain degree of control over others, or is responsible for organizing others, for the purpose of the criminal activity.²⁴⁵

In *Bermudez*, the authoritative command over co-conspirators, the recruitment of an accomplice, the supply of skimming devices to associates, and the use of the defendant’s computer to retrieve skimmed card numbers were considered to justify the application of the leadership enhancement under § 3B1.1(a).²⁴⁶ In *Mayans*, the court reasoned that defendant’s planning, the recruitment of a restaurant employee to use the skimmer, and the demand to a substantial share of the “fruits of the crime” fulfill the definition of the leadership role under § 3B1.1(c).²⁴⁷ In *Iyamu*,

²⁴¹ *Id.* at 605.

²⁴² *Id.*

²⁴³ U.S.S.G. § 3B1.1.

²⁴⁴ U.S.S.G. 3B1.1, cmt. 4.

²⁴⁵ U.S. Sentencing Commission, *Aggravating and Mitigating Role Adjustments Primer* 7-8 (March 2013), available at http://www.ussc.gov/sites/default/files/pdf/training/primers/Primer_Role_Adjustment.pdf.

²⁴⁶ *United States v. Bermudez*, No. 12-14250, 2013 WL 4750778 (11th Cir. Sept. 5, 2013).

²⁴⁷ *United States v. Mayans*, No. 10-10460, 2010 WL 3314480 (11th Cir. Aug. 24, 2010).

where the perpetrator enrolled and directed an individual for the criminal activity, the court of appeals held that the application of the § 3B1.1(c) enhancement was correct.²⁴⁸ In *Savarese*, although the defendant was not the conceiver of the criminal activity, the court reasoned that the form of authority does not need to be paramount or continuous, and, considering the defendant's activities, which included the recruitment of a co-defendant, the control of the information flow to his associates and the allocation of false identifications to co-conspirators, found that the defendant's level of authority sufficient for the application of the enhancement.²⁴⁹

E. Upward Adjustments

Courts may issue sentences beyond the U.S.S.G. range through departures or variances. A departure modifies the "final sentencing range computed by examining the provisions of the Guidelines themselves;" while an upward variance is a sentence imposed above "the otherwise correctly calculated sentencing range based on application of the other statutory factors in 18 U.S.C. § 3553(a)."²⁵⁰ According to U.S.S.G. § 5K2.0, a court may depart from the applicable guideline range in cases of unusual circumstances, of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines, in order to advance the objectives set forth in § 3553(a).²⁵¹ For instance, an upward variance was triggered in *Cowart*, where the court considered that the "cunning" employed, the monetary amount, and the "nearly continuous criminal activity" of the defendant support an upward sentencing adjustment.²⁵²

In *Roberson*,²⁵³ the defendant, following the accidental death of the person he was helping, concerned that he would face murder charges, concealed and burned the victim's body and did not report his death. Nevertheless, the defendant used victim's credit card repeatedly after the demise of the latter, claiming that he used the card with permission, and

²⁴⁸ United States v. Iyamu, No. 09-15534, 2010 WL 3279156 (11th Cir. Aug. 20, 2010).

²⁴⁹ United States v. Savarese, 686 F.3d 1, 20 (1st Cir. 2012).

²⁵⁰ U.S. Sentencing Commission, *Departure and Variance Primer* 1 (2013), available at http://www.ussc.gov/sites/default/files/pdf/training/primers/Primer_Departure_and_Variance.pdf.

²⁵¹ See Max M. Schanzenbach & Emerson H. Tiller, *Strategic Judging Under the United States Sentencing Guidelines: Positive Political Theory and Evidence*, 23 J.L. ECON. & ORG. 24 (2007).

²⁵² United States v. Cowart, No. 12-10382, 2013 WL 411345 (11th Cir. Feb. 4, 2013).

²⁵³ United States v. Roberson, 872 F.2d 597, 599 (5th Cir. 1989).

intended to repay the amount charged.²⁵⁴ The court, however, reasoned that the defendant's acts and omissions should be considered "extreme conduct," justifying the upward adjustment from the U.S.S.G. range of 30-37 months, and sentenced the defendant to 120 months in prison and two years' supervised release.²⁵⁵

In another interesting case under this category, in which the defendant was found in violation of 18 U.S.C. § 1029(a)(2), the prosecution requested an upward departure from the U.S.S.G. range, based on the assumption that the defendant had killed his wife, as "her death was the means by which he was able to perpetrated his crime."²⁵⁶ Based on findings such as the defendant's failure to report the disappearance of his wife to authorities, and that "he raided her accounts and credit cards by deception[,] either disguises or forgery[,] and he withdrew the daily limit of \$1,000.00 from her ATM— or from her bank's ATM over a period of about two weeks while wearing disguises", the district court reasoned that "causing death to effectuate the fraud scheme is sufficiently outside the heartland of the fraud, forgery, and false statement offenses to warrant a departure from the sentencing guidelines," and, citing § 5K2.1 of the U.S.S.G., imposed a sentence of 262 months, while the U.S.S.G. recommended a sentence of 41-51 months.²⁵⁷

The defendant, however, was never charged with the murder of his wife, and appealed the sentence. The court of appeals reasoned that, while the defendant benefited from the disappearance of his wife, the circumstances of her disappearance are unknown, and, even though the defendant may have been "played a causative or concealing role" in his wife's disappearance, there is no evidence as to the defendant's involvement.²⁵⁸ Therefore, the court reasoned that the district court's finding is not supported by facts, and consequently the upward departure pursuant to § 5K2.1, was an "abuse of discretion."²⁵⁹

V. CONCLUSION

Credit card frauds are made possible by many factors, including

²⁵⁴ *Id.* at 600.

²⁵⁵ *Id.* at 612.

²⁵⁶ *United States v. Fitch*, 659 F.3d 788, 790 (9th Cir. 2011).

²⁵⁷ *Id.* at 794 ("a substantial increase may be appropriate if the death was intended or knowingly risked or if the underlying offense was one for which base offense levels do not reflect an allowance for the risk of personal injury, such as fraud").

²⁵⁸ *Id.* at 800.

²⁵⁹ *Id.* at 801.

use of vulnerable technology, insufficient security, and lack of consumer awareness. These offenses often involve extensive conspiracies, some very sophisticated, crossing over many jurisdictions, which are difficult to prevent or investigate. A very high level of credit card fraud can negatively affect the economic stability and the trust in this payment method; therefore the stakeholders ought to effectively address this phenomenon.

To effectively prevent and combat these frauds, it is necessary to acquire a holistic understanding of the nature of these crimes. This article, based on an extensive inquiry, presented the essential aspects of credit card fraud cases. The findings of this article extend the understanding of credit card frauds and provide several practical implications for the stakeholders. The findings strongly suggest the need for improved legislative, judicial, and security measures.

Explicitly, it is imperative to mandate stronger standards and practices regarding the identity verification, the card number generation, the card delivery and activation, and the fraud detection. It is also indispensable to mandate effective security measures, even if the cost of such measures can be very high, in certain circumstances even surpassing the fraud losses. Deficiencies in this area could even amount to aiding or abetting the perpetrators.

The sentencing guidelines could be improved, to avert overbroad provisions, subjective interpretations, and excessive sentencing. Specifically, guidelines should allow for the easy distinction between the more culpable or dangerous perpetrators from the others, taking into account only the actual loss for the purposes of sentencing, and more carefully consider what should be construed as “sophisticated means.” Nonetheless, considering the high level of threat posed by the malicious software, the production, possession, use, or trafficking in such programs, with intent to defraud, should further increase the offense level.

It is also necessary to mandate federal or industry standards for secure coding and comprehensive software testing, the encryption or tokenization of transmitted or stored credit card data, the use of intrusion detection systems and security audit, and stronger access control, including the use of the multi-factor authentication mechanisms. Furthermore, as the magnetic strip technology is very vulnerable to counterfeiting and skimming, there is a clear need to globally implement the embedded-chip technology. Finally, credit monitoring, security freezes, and fraud alerts must be widely implemented and easily accessible.