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**

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

Ioana Vasiu* and Lucian Vasiu

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. Vasiu, Faculty of Law, Babeş-Bolyai University, e-mail: ioeav3@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 PGE 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. The main benefits of
electronic payments can be outlined as reduced transaction costs and
payment collection, increasing the transparency of payments, macroeconomic efficiency, expanded consumer markets and banking
penetration, and increased capital turnover ratio.

Credit cards, despite the availability of a variety of electronic
alternatives, such as digital wallets, checkout services, 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_payment_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).


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).

currencies, remain a widely used payment method. 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. 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. This impressive usage, however, presents abundant criminal opportunities.

Although there are significant efforts and innovations, aiming to

---


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


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. Aarun & 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 members 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.

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. 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. A high level of credit card fraud can negatively impact consumers trust. Consumer trust is an important social capital indicator, a determining factor of economic growth, and a major factor in purchase intentions. This can damage the reputation of the brands, and

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).


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


19 See Chao-Min Chiu et al., Understanding customers’ repeat purchase intentions in B2C e-
reduce the use or acceptance of credit cards.\textsuperscript{20}

Particularly worrisome is the online victimization rate,\textsuperscript{21} as electronic commerce represents an increasing percentage of the overall trade,\textsuperscript{22} with credit card as an important method of payment.\textsuperscript{23} Moreover, in certain massive breaches\textsuperscript{24} where credit card data was compromised, customers sued companies.\textsuperscript{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

\begin{footnotesize}
\textsuperscript{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).


\end{footnotesize}
purchase sex toys for him, or OpRobinHood, where members of the Anonymous and TeamP0is0N hacking groups carried out unauthorized credit card transactions for the benefit of the poor. Credit card frauds can take highly elaborated forms, executed by globally active organized crime groups ("OCGs"), affecting a very large number of victims. Even more disquieting, there are cases where the criminal activity involved money laundering and reports stating that credit card frauds represent a funding source for terrorists.

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

---

32 See Dahlia 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). Section 1029 was enacted under the Credit Card Fraud Act (1984), part of the Comprehensive Crime Control Act of 1984, 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). For the scope of this study, the first five subsections of 18 U.S.C. § 1029 (a) are of

---


interest: (1) the knowing, with intent to defraud, production, use, or traffic in of one or more counterfeit access devices; (2) the knowing, with intent to defraud, traffic in or use of one or more unauthorized access devices 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; 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.

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”). The intent to defraud
involves defendant’s state of mind, and may be demonstrated by direct or circumstantial evidence.

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. 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. 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).

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. 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. 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.

Lack of intent to defraud may be claimed when the device in the defendant’s possession isn’t fully functional. In Kaba, 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

---

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.
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
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).
67 Id. at 1239.
68 Id. at 1240.
69 Id.
71 Id.
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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 \textit{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.\textsuperscript{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.”\textsuperscript{77}

To invalidate charges, the defendants also claim the “access devices” are not capable of being used. In \textit{Onyesoh}, for exemplification, the defendant was convicted under 18 U.S.C. \textsection 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.\textsuperscript{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.\textsuperscript{79}

\textsuperscript{73} \textit{Id.} at 639.
\textsuperscript{74} \textit{Id.}
\textsuperscript{75} \textit{Id.} at 640.
\textsuperscript{76} \textit{United States v. Taylor}, 945 F.2d 1050, 1051 (8th Cir.1991).
\textsuperscript{77} \textit{Ibidem.}
\textsuperscript{78} \textit{United States v. Onyesoh}, 674 F.3d 1157, 1160 (9th Cir. 2012).
\textsuperscript{79} \textit{United States v. Onyesoh}, No. 12-50363, 549 F. App’x 700, 701-02 (9th Cir. Dec. 13,
In *Miralles*, 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(c)(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.  

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. 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.

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). 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. 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. 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
(3) the probative value of the evidence must not be substantially outweighed by its undue prejudice. 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.

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.” Co-conspirators are responsible for the losses resulted from the reasonably foreseeable acts in the furtherance of their conspiracy.

The provisions of Section 1029 have extraterritorial application, 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.” In Ivanov, for example, the perpetrator was physically present in Russia, and used the computer there, as relevant to the case. 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.

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).
92 United States v. Steinberg, 62 F.2d 77, 78 (2d Cir. 1932).
94 Id.
III. PERPETRATION ASPECTS

Criminals effect fraudulent transaction to obtain cash advances\(^95\) or to purchase luxury goods (like diamonds\(^96\) 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 losses\(^101\); 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 receipts\(^106\) or store records. In Sandoval, for example, the co-conspirators lifted clientele books from luxury department stores, such as Neiman Marcus and

---


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


\(^100\) 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).


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

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.\textsuperscript{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,\textsuperscript{109} or paying for goods or services at various establishments,\textsuperscript{110} or captured by housekeepers from hotel guests.\textsuperscript{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.\textsuperscript{112}

Credit card numbers may also be obtained through false advertising\textsuperscript{113} 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.)\textsuperscript{114} or victim’s personal interests (like famous fashion models or actresses). Phishing can take several forms: e-mail;\textsuperscript{115} SMS (“SMiShing”); social networks;\textsuperscript{116} phony web pages.\textsuperscript{117}

\textsuperscript{107} United States v. Sandoval, 668 F.3d 865, 867 (7th Cir. 2011).
\textsuperscript{108} Id.
\textsuperscript{112} See United States v. Stepianian, 570 F.3d 51, 53 (1st Cir. 2009).
or placement of fake applications in app-stores, which can allow man-in-the-middle (“MitM”) attacks when financial transactions occur.\textsuperscript{119}

In a myriad of cases, credit card numbers, rightly named “the ideal illicit Internet commodity,”\textsuperscript{120} by their nature very easily transmittable globally, were obtained via carding.\textsuperscript{121} Darknet\textsuperscript{122} 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,\textsuperscript{123} Lampeduza Republic,\textsuperscript{124} Carder.su,\textsuperscript{125} Barbarossa,\textsuperscript{126} or other bulk Internet transactions.\textsuperscript{127}

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

\begin{thebibliography}{99}
\bibitem{120} See Internet facilitated organised crime, \textit{EUROPOL} 5 (2011), available at \url{file:///Users/josephmccarthy/Downloads/iocta.pdf}.
\bibitem{126} See Global Payments breach puts 1.5 million credit card numbers at risk, \textit{CONSUMER REPORTS}, April 2 (2012), available at \url{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
merchant\textsuperscript{129} or payment processor level,\textsuperscript{130} is another important credit card fraud vector.\textsuperscript{131} Vulnerability exploitation can commonly be encountered as the infiltration vector,\textsuperscript{132} such as attacks using the Transport Layer Security ("TLS") features of OpenSSL,\textsuperscript{133} or web-based attacks, such as Structured Query Language ("SQL") injections,\textsuperscript{134} Cross-Site Scripting ("XSS") or Cross-Site Request Forgery ("CSRF").\textsuperscript{135} SQL injections, for example, are also used for exfiltration, as a means to obtain cardholder data ("CHD").\textsuperscript{136} Especially dangerous are the "zero-day" ("Oday") vulnerabilities, which are not known to victims before the attack that exploits the vulnerability is carried out.\textsuperscript{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,\textsuperscript{138} or to install card payments for merchants and banks, up to 1.5 million card numbers may have been stolen from its database).

\textsuperscript{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).

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

\textsuperscript{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).


\textsuperscript{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.


\textsuperscript{136} Id. at 8-9.


\textsuperscript{138} See United States v. Warthen, No. 10-10093, 2010 WL 3069635 (11th Cir. Aug. 6, 2010)
exfiltration computer contaminants\textsuperscript{139} ("malicious software" or "malware"),
for a similar end result.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{143} Plentiful reports mention
sophisticated malware employed in the perpetration of credit card frauds,
such as Torpig,\textsuperscript{144} Blackshades,\textsuperscript{145} SpyEye,\textsuperscript{146} Citadel,\textsuperscript{147} POSCardStealer,
Alina, or ProjectHook,\textsuperscript{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.\textsuperscript{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.\textsuperscript{150}

The PoS attacks facilitate the obtaining of massive amounts of credit card numbers. In Guvercin,\textsuperscript{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.\textsuperscript{152}

In certain extensive cases, millions of credit card numbers are compromised.\textsuperscript{153} The quintessential case in this regard can be considered Gonzalez,\textsuperscript{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.\textsuperscript{155} The malicious software allowed the capture of

\begin{itemize}
\item \textsuperscript{148} See McAfee Labs, supra note 124, at 6.
\item \textsuperscript{150} Id.
\item \textsuperscript{151} United States v. Guvercin, 10 Cr. 1206-01 RWS, 2013 WL 466429 (S.D.N.Y. Feb. 7, 2013).
\item \textsuperscript{152} Id.
\item \textsuperscript{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.
\item \textsuperscript{155} See United States v. Yastremskiy et al., 08-160(S-I)(SJF), 2008 WL 3199939 (E.D.N.Y. May 14, 2008) (superseding indictment).
\end{itemize}
track 2 data, transmitted from the compromised servers, via the system at D&B headquarters, to the data processor’s computer system.\textsuperscript{156}

Card numbers are used in numerous cases to clone\textsuperscript{157} legitimate cards, by encoding cards with perpetrator’s name.\textsuperscript{158} Credit cards, however, can also be counterfeit through other methods, including altering or forging. In Meredith,\textsuperscript{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.\textsuperscript{160}

\textbf{B. Physical Obtaining of Cards}

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

\begin{itemize}
\item \textsuperscript{156} \textit{Id.} at 4.
\item \textsuperscript{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).
\item \textsuperscript{159} Id.
\item \textsuperscript{160} Id.
\item \textsuperscript{162} Id.
\item \textsuperscript{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,\textsuperscript{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.\textsuperscript{167}

There are scores of cases where credit cards were obtained and used through various forms of identity theft.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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,\textsuperscript{171}

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). In Auguste, 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, 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, the perpetrator created fake identification documents and sold the documents to individuals who obtained credit cards based on those materials. In Madera, 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, perpetrators applied for instant credit based on credit reports acquired from legitimate businesses. In Maurello, 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, 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, perpetrators exploited “files” 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

---

173 United States v. Auguste, 392 F.3d 1266 (11th Cir. 2004).
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).
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. In Cantey, perpetrators opened credit accounts using the personal information of defunct or elderly victims. In Akinkoye, 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. As a number of his clients were women, he recruited Afolabi, who provided her photo for the identification associated with the cards.

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. 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.” 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, 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, 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, the perpetrator, a store employee, obtained, without authorization, copies of card numbers, afterwards used to

---

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).
fund his debit card and to order goods. In *Braggs*, 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*, 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*, for exemplification, the defendant, owner of a clothing business, placed tens of thousands of unauthorized charges, totaling millions of dollars. In *Catching*, 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”)* to the providers of the fraudulent or unauthorized cards.* In *Ismoila*, 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” despite being although non-

---

192 United States v. Braggs, 511 F.3d 808 (8th Cir. 2008).
195 United States v. Catchings, 708 F.3d 710, 714 (6th Cir. 2013).
198 United States v. Ismoila, 100 F.3d 380, 386 (5th Cir. 1996).
mandatory recommendations. 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,” and is the greater of actual loss or intended loss. In the case of stolen or counterfeit credit cards, the loss calculation considers at least $500 per access device. The loss calculation “does not have to be rigorously precise, only reasonable given the information available.” 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.”

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.” 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.

---

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 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”).
207 Id.
A different approach can be found in Barry, 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.” 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.

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. 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. Therefore, the case was remanded for resentencing. In Watt, the defendant adapted a sniffer program, subsequently used by the co-conspirator Gonzalez to obtain credit card numbers from TJX. U.S.S.G. holds the defendants accountable for “all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused” and for “all reasonably foreseeable acts and omissions of others in furtherance of the jointly undertaken criminal activity.” Consequently, the defendant was held “responsible for the entire loss, as an initial matter.”

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.” He

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.
216 U.S.S.G. § 1B1.3(a)(1)(B).
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 victims\(^ {221}\) 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”).


\(^{223}\) 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.\textsuperscript{226}

In \textit{Conner}, the defendant argued that, as all accounts were fully refunded for the unauthorized charges, cardholders could not be counted as victims.\textsuperscript{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.\textsuperscript{228}

\textbf{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.”\textsuperscript{229} While the ability to hack into order logs in order to obtain card numbers, and to rewrite CGI scripts,\textsuperscript{230} or the use of advanced skimming technology,\textsuperscript{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.\textsuperscript{232} This enhancement is also controversial because it allows for a double

\textsuperscript{226} \textit{Id.} at 1362.
\textsuperscript{227} United States v. Conner, 537 F.3d 480, 488 (5th Cir. 2008).
\textsuperscript{229} U.S.S.G. § 2B1.1 cmt. n.9 (2014).
\textsuperscript{230} See United States v. Prochner, 417 F.3d 54 (1st Cir. 2005).
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.  

Even in cases where no action is especially complicated or entangled, the series of criminal actions may be construed as “sophisticated means.” 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. 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.

In Jackson, 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.” 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.”

In Calhoun, 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,
they argued that what they did was “a garden variety offense.” 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.

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).” 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.”

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. 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).

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). In Iyamu,
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.\footnote{United States v. Iyamu, No. 09-15534. 2010 WL 3279156 (11th Cir. Aug. 20, 2010).} 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.\footnote{United States v. Savarese, 686 F.3d 1, 20 (1st Cir. 2012).}

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).”\footnote{U.S. Sentencing Commission, Departure and Variance Primer 1 (2013), available at http://www.ussc.gov/sites/default/files/pdfs/training/primers/Primer_Departure_and_Variance.pdf\footnote{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).}} 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).\footnote{United States v. Cowart, No. 12-10382, 2013 WL 411345 (11th Cir. Feb. 4, 2013).} 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.\footnote{United States v. Roberson, 872 F.2d 597, 599 (5th Cir. 1989).}

In Roberson,\footnote{United States v. Roberson, 872 F.2d 597, 599 (5th Cir. 1989).} 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
intended to repay the amount charged.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.”\textsuperscript{259}

\textbf{V. CONCLUSION}

Credit card frauds are made possible by many factors, including

\begin{flushright}
\textsuperscript{254} \textit{Id.} at 600.
\textsuperscript{255} \textit{Id.} at 612.
\textsuperscript{256} United States v. Fitch, 659 F.3d 788, 790 (9th Cir. 2011).
\textsuperscript{257} \textit{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”).
\textsuperscript{258} \textit{Id.} at 800.
\textsuperscript{259} \textit{Id.} at 801.
\end{flushright}
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.