2016

The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?

Maria Tcherni-Buzzeo
University of New Haven, mtcherni@newhaven.edu

Andrew Davis
State University of New York Albany

Giza Lopes
University of Albany

Alan Lizotte
University of Albany

Publisher Citation

Tchweni-Buzzeo, M., Davis, A., Lopes, G., Lizotte, A. (2016). "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" Justice Quarterly 33(5):890-911 doi: 10.1080/07418825.2014.994658

Comments

This is an Accepted Manuscript of an article published by Taylor & Francis in Justice Quarterly in August, 2016, available online: **http://www.tandfonline.com/10.1080/07418825.2014.994658**

Published online Jan. 8, 2015.

THE DARK FIGURE OF ONLINE PROPERTY CRIME:

IS CYBERSPACE HIDING A CRIME WAVE?

Authors: Tcherni, M., Davies, A., Lopes, G., & Lizotte, A.

Author bios:

Maria Tcherni, PhD, is an assistant professor of criminal justice at the University of New Haven, CT. She holds a PhD from the University at Albany (SUNY). Her research interests include explaining crime trends and patterns, unraveling structural and biosocial causes of violence, and testing criminological theories. She published in the *Journal of Quantitative Criminology*.

Andrew Lucas Blaize Davies, PhD, is a post-doctoral fellow at the State University of New York at Albany. His publications have appeared both in edited volumes and journals including Law and Society Review, Studies in Law, Politics and Society, and the Albany Law Review. In his professional capacity, he oversees a program of regular data collection and research into the provision of legal services to indigent persons in New York State.

Giza Lopes, PhD, is a Postdoctoral Associate at the School of Criminal Justice, University at Albany. She is primarily interested in policy research of issues lying at the intersection of health and criminal justice, particularly the medicalization of society and attendant legal shifts.

Alan Lizotte, PhD, is Dean and Professor in the School of Criminal Justice at the University at Albany. He is co-principal investigator on the Rochester Youth Development Study (RYDS), a 26-year ongoing longitudinal study of juvenile delinquency and drug use covering three generations of subjects. His substantive interests include illegal firearms ownership and use and developmental criminology. In 2003, together with his RYDS coauthors, he was awarded the American Society of Criminology's Hindelang Award for the book *Gangs and Delinquency in Developmental Perspective*.

Acknowledgement:
We gratefully acknowledge the huge role that meetings of the International Society on Life and Death Studies (ISOLADS) played in shaping this paper and forging the ideas underlying it. A preliminary version of the study was presented at the annual meeting of the American Society of Criminology in Atlanta, GA, in 2013. We thank the three anonymous reviewers for their careful reading and valuable suggestions during several rounds of reviews.

ABSTRACT

A pronounced drop in crime since the early 1990s has encompassed every crime category tracked by the FBI's Uniform Crime Reports, including property crime. However, over the same period, the rates of Online Property Crime (OPC) have been on the rise according to available evidence. We delineate the extent of our knowledge and data concerning cyber crime and identity theft and, using data from several nationally representative victimization surveys, offer an alternative view of property crime trends while pointing out the glaring gap in crime reporting and accounting in relation to the growing category of property crimes perpetrated online. In addition, we compare estimated costs of traditional property crime versus online property crime. Finally, we identify the main challenges for obtaining reliable data on online property crime and discuss their implications, especially when applying the traditional methods of compiling crime statistics.

INTRODUCTION: DID CRIME DROP OR DID WE DROP THE BALL?

A pronounced drop in crime since the early 1990s has encompassed every crime category tracked by the FBI's Uniform Crime Reports (Truman, 2011; U.S. Federal Bureau of Investigation, 2013). It has affected property crime (burglary, larceny/theft, motor vehicle theft, etc.) as well as violent crime (homicide, robbery, rape, etc.). Over the same period, the rates of internet-perpetrated crime – often in the forms of identity theft, fraud, and cyber-attacks on organizational computer networks, among others – have been on the rise according to available sources of data (Allison, Schuck, and Lersch, 2005; Langton, 2011; Newman, 2009a; Symantec, 2012; U.S. Federal Trade Commission,

2004, 2008, 2012). Notwithstanding these contrary trends, criminologists frame crime trends since the 1990s within the paradigm of a 'crime drop' (Blumstein and Wallman, 2005; Goldberger and Rosenfeld, 2008), and have generally neglected the possibility that official statistics are an increasingly incomplete reflection of the extent of criminal activity in the United States. This paper explores the implications of that possible omission.

In this paper, we delineate the extent of our knowledge and data concerning Online Property Crime (OPC) and offer an alternative view of property crime trends generally while pointing out the glaring gap in crime reporting and accounting in relation to the crimes perpetrated online, which are likely growing in number. In addition, we compare estimated costs of traditional property crime to those of OPC. Finally, we identify the main challenges in obtaining reliable data on OPC, especially when applying the traditional methods of compiling crime statistics. The framework offered in the current article challenges the traditional perception of property crime as following the same downward trend as violent crime. It is our hope that the discussion started here will facilitate efforts to gather relevant information to track the trends in OPC more accurately.

DEFINING AND COUNTING ONLINE PROPERTY CRIME[1]

We use the term Online Property Crime to cover a wide variety of property crimes perpetrated online including identity theft, credit card theft and fraud, cyber attacks on organizational networks resulting in security breaches, the buying and selling of personal

[1] We are grateful to one of our anonymous reviewers for raising several of the definitional points in this section.

data online, and the use of unsuspecting people's computers for spamming/phishing/illegal hosting (see Cheney, 2003, 2005; Anderson et al., 2012 for the discussion of definitions and types of online property offenses). Two aspects of this definition are worth highlighting: that OPC is perpetrated online, and that it involves the theft of property. We discuss the importance of these distinctions below.

Defining a crime as 'perpetrated online' is not a simple matter. Some types of OPC have a significant offline component. For example, identity theft and credit card fraud can and often do result from "dumpster diving", theft from mailboxes, or stealing relatives' personal information through paper documents (Allison et al., 2005; Elbirt, 2005; White and Fisher, 2008; Copes and Vieraitis, 2009; Morris, 2010). When fraudulent transactions are reported, it is often impossible to infer exactly how the information was obtained, or even how it was exploited. Accordingly, in our review of the data that follows, we are at pains to distinguish between sources which focus exclusively on crime perpetrated online, as our definition requires, and those which aggregate data on an overlapping, but distinct, quantity of criminal activity.

Establishing that property was taken in a perpetration of an online crime is also complex. If the 'property' at issue is a person's identity, a problem is created because some victims of online identity theft never become aware that their details have been stolen, and indeed do not lose their identity so much as 'share' it with the criminal. Others may have their details exploited to obtain products or services but will suffer no direct loss themselves – arguably a crime more similar to defamation than 'theft', at least as far as the original owner of the data is concerned. Equally, online property crime may result in no direct profit to the criminal in cases where, rather than seeking financial

payouts, the criminal steals intellectual property which may then be exploited in other ways. Accordingly, as we review the data that follows, we consider the types of property at issue and problems related to the quantification of property lost.

Additionally, other factors may bias or inhibit full documentation of OPC. Insurance company requirements that victims report losses to the police may bias data in favor of higher value losses, while the active encouragement to report fraud offered by websites such as eBay may have other skewing effects (see House of Lords Science and Technology Committee, 2007, p.110). Equally, changing technology itself may influence target selection by criminals. As Biderman and Reiss noted in 1967, crime data produced by organizations responsible for policing or adjudication "are not some objectively observable universe of 'criminal acts', but rather those events defined, captured, and processed as such by some institutional mechanism" (p. 1). Accordingly, we sought to remain continually vigilant of what is referred to elsewhere as the 'dark figure' problem – that is, factors that cause reported statistics to diverge from (and generally underrepresent) the true nature and extent of crime.

Notwithstanding these significant challenges, there is a pressing need to count online property crime for two reasons. First, it is likely that it is increasing. Internet usage has increased dramatically in the United States in recent decades, such that in September of 2012, 81% of American adults and 95% of teens accessed the internet (Pew Research Center, 2013). This change can be reasonably compared to other expansions of human activity through time and space. Melbin (1978) showed how the expansion of human activities past dusk, facilitated by the introduction of electric lighting into newly

settled territories in the West, had an impact on crime. Every time human activity crosses new 'frontiers', crime seems to follow.

Second, the potential harm from OPC is unknown. In the case of property crime, 'harmfulness' is almost always quantified in terms of the financial losses accrued by the victim (Davies, 2012). Data on losses from property crime are, in fact, regularly published by the FBI, though no facility is provided to allow a breakdown of online vs. offline crimes which, alongside other concerns about the representativeness of the FBI's data, makes it impossible to check how much harm OPC is causing or to relate it to more familiar measures such as the financial harm caused by other thefts. Accordingly, rendering a reasonably satisfactory picture of the quantity of financial losses that accrue from OPC is critical to our ability to track its seriousness as a social problem.

Detecting the 'true' extent of OPC poses questions that are not only conceptual, therefore, but also methodologically technical. In what follows, we consider specifically the limitations of official statistics, victimization surveys and other approaches to data collection when applied to the problem of counting OPC in order to make the case that greater attention should be devoted to assessing the harmfulness and prevalence of OPC in the United States.

THE SIZE OF THE PROBLEM: HOW PREVALENT IS OPC?

At the same time as traditional property crime has fallen nationally, the online market for personal and financial data has formed (see Holt and Lampke, 2010 for an empirical study of such online marketplaces). After 2004, according to Moore and his colleagues (2009), identity theft and credit card fraud became increasingly organized and

elaborate, evolving from a problem of 'insiders' with access to sensitive information (such as store attendants) to one with a novel division of labor. *Phishermen* (and sometimes *spammers*) would send out emails and viruses to attract naïve customers to fake bank web sites requesting a person to enter their bank account number and password for 'confirmation' or to avoid 'suspension of the account'. *Botnet herders* would manipulate infected computers to gather keystroke information and to direct these computers – unbeknownst to their owners – to execute specific programs, host fake web sites and online pharmacies, and send out spam emails. *Brokers* and *cashiers* would buy bank account information in bulk and would in turn hire unsuspecting *money mules* (through job advertisements for positions of 'transaction processor' or 'account executive') to accept money transfers from these stolen bank accounts into their own accounts, keep a commission, and then irretrievably transfer the rest of the money through Western Union (or other untraceable means) to the *cashiers* (Moore, Clayton, and Anderson, 2009). In 2011, Symantec reported the price for 10,000 bots (infected computers acting as 'robots' on commands) was around $15, while stolen credit card numbers could fetch between $0.07 and $100 each (Symantec, 2011, p. 6).

When it comes to understanding the scope and incidence of conventional, non-online crime types, criminal justice researchers and professionals have several options. Traditional ways of measuring crime include official statistics from the FBI's Uniform Crime Reports (UCR), victimization survey data (from both individuals and businesses affected), and self-reported crime and delinquency from various sources (though there is no uniform nationally representative survey of self-reported crime involvement with large samples of adults – see Addington, 2010, for an overview.) Of the three main sources of

crime measurement, official statistics and victimization data are, at least in theory, most relevant for providing information about the extent of OPC. Additionally, these are the only sources of data that presently have the potential to derive national estimates of the scope of the problem in the United States.

The differences between measures of crime reported to (and by) the police reproduced in the FBI's Uniform Crime Reporting (UCR) program and measures of victimization gleaned from NCVS have been analyzed and dissected extensively (Biderman and Lynch, 1991; Loftin and McDowall, 2010; Lynch and Addington, 2007; Mosher, Miethe, and Phillips, 2002; Savitz, 1978; Skogan, 1977, 1984; Xie et al., 2006; Zawitz et al., 2003). This literature has two lessons with particular relevance for interpreting data in relation to OPC. First, existing research shows consistently that a much smaller proportion of victims of property crime report their victimization compared to victims of violent crime. Second, the most prominent reasons that victims of property crime do not report their victimization are threefold: the crime or its resultant losses are minor enough that they are not worth the time and effort of reporting, the property was recovered, or victims do not believe police could help recover the property (Skogan, 1984; Harlow, 1985; Hart & Rennison, 2003). Accordingly, when assessing the validity of data on the prevalence of OPC nationally, existing research suggests strongly that the extent of the problem will be underestimated in official statistics (White & Fisher, 2008), and that there will be an overrepresentation of high-loss crimes[2].

[2] There is also a possibility that the need to create a record of a crime for insurance purposes will play an important role in biasing the types of crimes reported, though we note there is only limited evidence for the importance of insurance as an incentive to report crimes in other areas (Skogan, 1984; Harlow, 1985; Hart & Rennison, 2003).

According to the broad consensus among criminology researchers, backed up by the UCR reports, property crime has been declining since the early 1990s in the United States (Blumstein and Wallman, 2005; Levitt, 2004; Mishra and Lalumière, 2009; Zimring, 2006) as well as internationally (Mishra and Lalumière, 2009; Tseloni et al., 2010). Of course, OPC does not appear as a specific category in the Uniform Crime Report estimates compiled by the FBI, upon which so much research and speculation regarding crime trends are based (U.S. Federal Bureau of Investigation, 2013). Rather the observation of this decline in property crime is based on counts of burglary, larceny-theft, motor vehicle theft, and (to a limited extent) arson.

Several explanations have been offered to account for the overall crime decline. Levitt (2004) summarized the most commonly cited hypotheses for the fall in crime rates: increased imprisonment; the aging of the population (i.e., the drop in the proportion of high-risk youth); improved economic conditions; innovative police strategies (e.g., 'hot spots' and 'community policing'); changes in gun control laws; increased use of the death penalty; increased numbers of police officers; the legalization of abortion and attendant reduced number of unwanted, at-risk children; and the decline in crack-cocaine consumption. Levitt's list is not exhaustive; others have suggested that growths in immigration may account for a reduction in crime (Wadsworth, 2010), particularly violent offending, or that changes in "youth culture," observed by qualitative researchers in inner-city neighborhoods, may also explain the crime drop (Curtis, 1998). While a few of these explanations find more empirical support than others, in reality the crime decline debate remains largely unresolved and the trends are "murkier" than much of the existing literature suggests (Baumer and Wolff, 2014).

Data from the National Crime Victimization Survey (NCVS) tend to confirm the downward trend as well: in the United States, "[p]roperty victimization [in 2010] fell to the lowest levels since 1993" (Truman, 2011, p. 7). Questions about the experience of identity theft, defined as an unauthorized use of an account, an unauthorized attempt to create a new account, or another fraudulent use of personal information, were only added to the National Crime Victimization Survey in 2004, however, and thus trend data only exist for the period after the most dramatic crime decline had happened (Baum, 2006; Harrell & Langton, 2013). According to the NCVS estimates, the number of households affected by identity theft has risen from 3.1% in 2004 to 7% in 2010, while the number of individuals affected rose from 5% of the population in 2008 to 7% in 2012 (See Table 1; Baum, 2004; Langton, 2011; Langton & Planty, 2010; Harrell & Langton, 2013). At the same time, Piquero and her colleagues concluded that the "number of households being victimized annually rang[es] between 5% and 25%" (Piquero, Cohen, and Piquero, 2011, p. 437). These figures do contain some indication that identity theft rates are rising (see Table 1). Regrettably, however, neither source collected information regarding the mode of perpetration of the crimes in question.[3]

The other nationally representative data source on identity theft, credit card fraud, and other forms of online fraud victimization is a longitudinal survey launched in 2003–2004 by Javelin Strategy & Research, a private company (see Javelin, 2009). The sample is a nationally representative rotating sample of about 5,000 U.S. adults, and the survey is

[3] It is important to underscore a critical difference in the ways the prevalence of online property crime is measured in available sources. Whereas the NCVS measures the 'number of victimizations' per 100 individuals aged 12+, the data do not account for whether the same or different individuals were victimized. As a result, the numbers do not actually tell us what percentage of individuals are affected by online property crime, but only the rate at which victimization incidents occurred. The best estimates for the rates at which people are actually affected by online property crime suggest it affects between 4.4% and 6.0% of the adult population annually (Javelin Strategy & Research, 2012), or between 5.5% and 7.3% of households nationally, according to NCVS data (Langton, 2011).

conducted annually. Reports detailing the results of the survey have been issued every year since 2005 (see Table 1).

[Table 1 about here]

Javelin sought to break down its 2008 data on identity theft by method of perpetration, an effort which was hampered by the fact that 65% of victims in that year did not know how their information had been obtained (Javelin, 2009). Only 4% of victims knew they had lost their data online, while a further 4% believed it had been lost through a data breach. Meanwhile, fully 15% believed their identities had been compromised after their wallet was stolen. Javelin's conclusion, that most identity theft occurs offline, was in line with other research, but suffers from the flaw that victims of OPC are far less likely to know or understand how their information was compromised than are victims who are aware they lost their wallets.

Fewer than 20% of the identity theft victims sampled by NCVS reported their victimization to law enforcement agencies (Langton and Planty, 2010).[4] A similar estimate of reporting rates is derived by Copes and his colleagues (2010) from the second wave of a nationally representative National Public Survey on White Collar Crime conducted by the National White Collar Crime Center (NW3C) in 2005. That survey found that 19.6% of identity theft and credit card fraud victims in their sample reported their victimization to a crime control agency (Copes et al., 2010, p. 1048). Results from the third wave of that survey, conducted in 2010, suggested 26% of victims of identity

[4] Interestingly, the U.S. Department of Justice has a section on their web site titled "What Should I Do If I've Become a Victim of Identity Theft?" It advises victims to report their victimization to the U.S. Federal Trade Commission (FTC) and several other organizations (for example, Internal Revenue Service, Social Security Administration, and credit reporting companies) but reporting to the police is not included in that list. (http://www.justice.gov/criminal/fraud/websites/idtheft.html, accessed 8/14/14).

theft or credit card fraud reported their victimization (Huff, Desilets, and Kane, 2010, p. 16).

[Table 2 about here]

Table 2 summarizes the estimates of reporting to police derived from NCVS and the NW3C survey and compares them to the reporting of traditional property crime to police (based on NCVS data). Identity theft victimization is reported to police at a significantly lower rate – around 20% – compared to the proportion of people who report their victimizations from traditional property crime to police – about 40%, according to NCVS data (Truman, 2011). Moreover, one important consideration makes this difference in reporting a conservative estimate: neither NCVS nor the NW3C survey separate identity theft that is perpetrated online from that which results from "dumpster diving" or stealing mail from mailboxes. The real gap in reporting between OPC and traditional property crime may be even wider.

Data from the U.S. Federal Trade Commission (FTC), supplied by victimized consumers on a voluntary basis, help to add further insights when juxtaposed with those from NCVS (U.S. Federal Trade Commission, 2004, 2008, 2012). According to the FTC data, the percentage of people victimized by identity theft or fraud who notified police varied between 35% and 49% for the years 2001–2008. An actual police report was filed in between 27% and 40% of cases depending on the year (see Table 2). However, the FTC data, besides having the same problem of non-separation of online crimes, also have another serious flaw: they clearly cannot be considered representative of all victims of fraud and identity theft, but rather represent (at best) only those individuals reaching out

to the data collection agency.[5] The most that can be said for these data, therefore, is that among those who take the step of voluntarily reporting their victimization to the FTC, reporting to the police also appears more common.

Victims of internet-based crimes also have a separate venue for reporting: the Internet Crime Complaint Center (IC3) where complaints can be filed online and annual reports are produced summarizing the information received from the reporting victims (see the latest report in Internet Crime Complaint Center, 2013). These data seem to be useful for detecting certain fraud patterns and new fraud scenarios, which is helpful for law enforcement in connecting cases. IC3 data are also helpful in issuing warnings to consumers about the emerging threats and online frauds. At the same time, these data are much less useful in piecing together a comprehensive picture of online crime since the questions about the generalizability arise with IC3 data just as much, if not more, than with the FTC data. For example, plenty of complaints filed through IC3 are related to online auctions, which may be a result of eBay's encouragement of its consumers to report to IC3 (see House of Lords Science and Technology Committee, 2007, p.110).

In sum, the picture from available data sources suggests that OPC affects a sizeable and growing proportion of households annually in comparison to traditional property crime, but that reporting rates to police are relatively low. Moreover, OPC levels and trends are not counted at all in the FBI's UCR metric, which is most commonly used to assess crime levels and trends in the United States. Rather, the only

[5] In addition, over the years of data collection, fewer and fewer consumers answer the question about reporting their victimization to police (less than half of people reporting their victimizations to FTC provided an answer about reporting it to police in 2009, 2010, and 2011), thus further undermining the generalizability of FTC data.

available sources for national estimates of the prevalence of the problem are victimization surveys. Next, we assess the level of damage that OPC precipitates on its victims.

THE SERIOUSNESS OF THE PROBLEM: HOW MUCH DOES OPC COST?

Estimates of financial losses from online theft and fraud are compiled by Javelin Strategy & Research (2011), using a methodology closest to the one employed in calculating losses from traditional crime by the FBI in their annual Crime in the United States reports (U.S. Federal Bureau of Investigation, 2013). The results paint a picture that clearly shows losses from online crime far surpass those from traditional crime (see Table 3) and that the proportion of people or households financially affected by OPC is substantial.

[Table 3 about here]

By asking respondents to identify the date of their discovery of the loss and the 'approximate total dollar value of what the person obtained while misusing information', Javelin computes a moving three-year average of monetary losses (except for years 2008 and 2009, where only a standard one-year estimate was available at the time of report publication). As can be seen from Table 3, the total losses vary within the range of $45 billion to $60 billion yearly during the period of 2003–2009. Table 3 also includes direct personal financial losses from identity theft, estimated using NCVS: these ranged from $14.4 billion to $16.5 billion annually over the same period of time. UCR estimates of monetary losses reported from the traditional property crimes such as burglary, larceny/theft, and motor vehicle theft, by comparison, range between $15.2 billion and $17.6 billion.

Three important considerations should be kept in mind when comparing these three sources of data on financial losses from property crime. First, the estimates from Javelin Strategy & Research include the losses borne out by the industry (banking institutions and merchants), whereas data from NCVS only include financial losses borne out by the private individuals. The lack of awareness among victims may mean the actual value of financial losses is higher, though difficult to estimate.[6] According to the estimates by Gordon and his colleagues (2007), individuals constitute only approximately 34% of the victims of identity theft, with financial industry organizations constituting over 37% of the victims, and retail businesses representing 20% (Gordon et al., 2007, p. 3). Thus, individual victimizations only represent the tip of the iceberg in terms of financial losses. Different methodologies of calculating losses and different definitions of online crime (identity theft, credit/debit card fraud, etc.) lead to different estimates of per person and overall losses. Moreover, surveys of individuals can bias estimates of losses upwards if the percentage of population affected is small and may not be represented well, even in fairly large samples (see Florêncio and Herley, 2013, for an excellent discussion of this issue). Taking these considerations into account, even if upwardly biased, the survey estimates could result in a figure that is a closer reflection of real losses to the industry.

Second, the UCR estimates include financial losses from property crime against both individuals and organizations but only from the crimes that were reported to the police. Even though only less than half of all property crime is reported to the police

[6] As an example, based on a series of studies commissioned by Symantec and conducted by the Ponemon Institute (2012) where large U.S. companies (over 2000 employees per company) were surveyed, the average financial loss from data breach incidents per year per company is estimated to be $8.9 million. However, this estimate cannot be easily translated into a national total because of the method by which the sample was drawn.

(according to NCVS estimates), the figures for financial losses cannot be assumed to be representative of losses for all such crimes because one of the main reasons some property crimes are not reported to law enforcement is the insignificance of losses (as described above, in the section on prevalence of OPC). However, to adjust for this possibility, a crude estimate is offered in Table 3 as a proxy – the doubling of the officially reported losses. Even adopting this liberal approach, which likely overstates the true amount of total losses from traditional property crime adjusting for non-reporting, the resulting estimates are still much lower than the estimated direct losses caused by identity theft (see Table 3).

To summarize, the financial losses attributable to identity theft appear far in excess of the damage inflicted by traditional property crime, though there is no clear indication of the role of online perpetration in these data, or of whether levels of online perpetration are rising or falling in recent years. Nevertheless, we believe the data reviewed above do constitute a *prima facie* case that OPC rates and losses may be comparable to, or even greater than, those from traditional property crime in recent years.

PUZZLE FOR THE NEW AGE: HOW SHOULD WE COUNT ONLINE PROPERTY CRIME?

The UCR was designed to count the kinds of direct contact predatory crimes typical of the 1940's and 1950's, where victims and offenders came together in time and space. Today, victims and offenders can meet in cyberspace and the authorities that may be able to do something about it are often private corporations rather than police, who have traditionally generated crime statistics. The possibility arises that the crime drop is a

consequence, in part, of an incremental shift of criminal behavior out from under police surveillance or auspices, and into the online realm. Present data render this proposition untestable, but of critical importance to researchers.

Given the substantial number of people affected and the huge amounts of financial losses caused, as well as the organized nature of crime markets for online theft, the U.S. criminal justice system needs a better way to incorporate information about OPC into its statistics on trends and patterns of crime. It's dangerous for researchers to come up with explanations for the crime drop by building theories based on assumptions about the nature of crime that are increasingly outdated, because the trends in criminality may be incorrectly described. The implication is a profound one: widespread criminological concern about the 'crime drop' may be based on misconceptions about the extent or even the existence of that drop itself. Next, we contemplate the challenges that will beset any attempt to incorporate online property crime into generalized crime measures.

Most attempts to count crime involve making the critical decision to count either incidents of offending or victimization, and OPC is no exception.

[Table 4 about here]

One successful security breach of a network may only be a single offense, but its effects on victims may be widespread if millions of data records containing personal information are accessed by the hackers. Such a crime may expose millions of people to becoming potential victims of identity theft or account fraud (see Table 4 for the incidents with the largest volumes of financial/personal information exposed). Yet each data breach incident of this kind may be perpetrated by just a few offenders, or only one offender may be involved at the initial stage. Thus, depending on what one counts, the

numbers of offenses may differ from the number of offenders or victims by orders of magnitude.

Among traditional types of crime, very few are characterized by such a massive asymmetry between the numbers of offenders and victims. A rare exception to this rule is Bernie Madoff's 'Ponzi scheme', which is an unusual example of a traditional property crime of fraud. In that extraordinary case, thousands of individuals, plus thousands of organizations, can be counted among the victims while there are only a handful of offenders. It seems that separate (and often very disparate) counts need to be compiled for victims, offenders, incidents, and financial losses, each of which might be considered a valid measure in the context of an attempt to measure the extent of crime and the harm it causes. Below, we will consider each of these categories and describe possible solutions for counting.

Data on OPC offenders are, if anything, likely to be the hardest to calculate. The time and space constraints (Cohen and Felson, 1979) that govern most of the traditional crime are substantially relaxed for OPC. Offenders may, and often do, reside in other countries halfway across the globe, whereas victims may be U.S. residents and businesses. Such crimes are particularly hard to solve, making data collection on offenders very complex. While certain offenders may be caught and portrayed in media, the profile of such individuals is likely to be highly unrepresentative of offenders generally. In short, data on offending itself is likely to be very hard to come by, and may transgress certain assumptions that underlie the attempt to produce a 'national' estimate of OPC prevalence.

The counting of victims also poses conceptual challenges. According to Newman (2003), "over 90% of people report their lost or stolen card to the card issuer within one day" (p. 8). In such cases, if a person suffered no financial losses because the credit card company reversed any unauthorized charges, can the credit card holder be considered – and counted as – a victim of OPC? Does it depend on whether the person was even aware of the unauthorized charges? What if s/he was made aware of the situation only after the credit card company resolved the issue? The parallel with traditional types of crimes would be an 'attempted' crime. Should we then consider the individuals exposed to OPC but bearing no financial damage as 'potential victims' or 'victims of attempted crime' and only count the credit card company as an actual victim? Additionally, how is one to classify the victim whose financial information is stolen but never exploited, for whatever reason? Measures of victimization are particularly ineffective around incidents such as those where the putative 'victim' either suffers no harm at all, or is unaware of what has happened. These are the questions that need to be resolved for the purpose of developing a system of consistent OPC data.

An additional challenge results from the fact that businesses affected by OPC may be unwilling to come forward with information, in the effort to preserve their reputation and their customers' trust:

> Banks and creditors typically do not notify the police about identity thefts, and police do not contact banks and creditors—and even if police did contact banks and creditors, there are no established procedures for the transfer of relevant information. […] In fact, there are indications that the private sector would rather keep this type of identity theft private, electing to address the control of the problem on its own. Many credit card companies and financial institutions view identity theft through a cost-benefit analysis, and the costs of implementing anti-identity theft measures exceed their benefits. (White and Fisher, 2008, p. 10)

Other researchers also confirm the desire to conceal commercial victimization through data breaches (Clarke and Newman, 2002; Smith, 1999; Taylor, 2002), and add that managers may doubt the ability of police to deal with the crime, which would require technologically advanced knowledge or equipment.

As a partial remedy for this problem, data breach laws requiring businesses to report any substantial security breaches have been passed in almost all U.S. states in the last 10 years, starting with California that passed the first law of this kind in 2002. As of April 2014, 47 states – with the exception of Alabama, New Mexico, and South Dakota – had enacted security breach laws (National Conference of State Legislatures, 2014). As a result, the reporting of security breaches has improved (for more on the effectiveness of data breach laws, see Romanosky et al., 2011).

There is also a centralized database provided by a non-profit organization relying on volunteers that accumulates information on security breaches and on the number of personal and financial records exposed to online theft – DataLossDB.org project (Open Security Foundation, n.d.). Figure 1 plots the DataLossDB records of reported data breach incidents on a timeline: monthly number of incidents from 2005 to mid-2014 (latest available when the article went to press), regardless of the number of records stolen or exposed in each incident. In the period between 2009 and 2013, the increase looks exponential. Symantec (2012) estimates that in 2011, on average, 1.1 million identities got exposed per breach incident (p. 9), compared to 260,000 in 2010 (Symantec, 2011, p. 6).

[Figure 1 about here]

Finally, when it comes to counting losses from OPC, the problem is similar to that of arson: sometimes, arson results in very little damage (if fire does not spread or is put out quickly) and sometimes damages run into millions of dollars. Often, external factors which have nothing to do with the offenders or their intent determine the amount of losses. To resolve (or rather avoid) this problem, UCR data on property crime exclude arson all together from loss calculations. For OPC, the amount of actual losses can be calculated only if a mechanism is developed to gather information from both individuals and organizations. However, a mandatory reporting system for financial losses is very unlikely to be implemented unless the government provides a financial incentive to disclose this information (for example, in the form of tax breaks or loss write-offs tied to the requirement of mandatory disclosure). Another possible solution to this problem can come in the form of mandatory insurance against online fraud that would be required of any businesses with substantial online presence or possibility of exposing customer data through online security breaches. A certain level of online security would be required to purchase the insurance (with discounts for a higher level of security) and the reporting of security breaches (to the insurer or to special investigative divisions) would be a mandatory requirement for collecting on the insurance. This method might ensure high rates of reporting – similarly to what we see with motor vehicle theft (according to the U.S. Federal Bureau of Investigation (2013), the theft of motor vehicles is one of the most consistently highly reported property crimes).

Otherwise, the only viable option of gathering data on organizations' financial losses from OPC is the one that has been implemented by the Bureau of Justice Statistics (BJS) in collaboration with the RAND Corporation in the National Computer Security

Survey (NCSS) (Bureau of Justice Statistics, 2006). The survey has been devised to collect information from business organizations about their cybercrime victimization experiences. Despite the strong sampling procedure that was intended to produce solid national estimates (a stratified, random sample of nearly 36,000 businesses was selected), the response rate to this survey was only about 23%. Such a low response rate calls into question the generalizability of any estimates obtained from the survey, especially since it is not clear whether the businesses that responded were more or less or equally likely to be victimized compared to the businesses that gave no response to the survey.

It is also important to make a distinction between two types of cybercrime against organizations: 1) malicious attacks that are most similar to vandalism – computer viruses, denial of service, and other attacks designed to bring damage to the systems without the intent to profit financially from such damage, and 2) cybercrime that is perpetrated with the explicit intent to profit (designated as cyber theft in the BJS report (Rantala, 2008)). These two types of OPC (cyber-vandalism and cyber-theft) may have very different origins and types of perpetrators but both cause substantial financial losses to the organizations targeted.

CONCLUDING THOUGHTS: THE COUNTER-TRENDS AND INVISIBLE LINKS

While data and research in the area are incipient, the analysis above suggests there is ample reason to devote greater attention to counting OPC in order to assess whether the explosion in online property crime in the United States is so great as to reverse the commonly observed 'crime drop' since the mid-1990s. The data presented here suggest that the rate at which United States residents are now affected by OPC actually outstrips

that of traditional property crime, which continues to fall. Moreover, the amount of financial harm they suffer is far greater in dollar amounts than that inflicted by traditional property crime. Existing data allow us to suggest the possibility that this 'wave' in crime may override any benefits Americans have enjoyed as a result of the steady drop in traditional forms of property crime recorded in the UCR.

The counting of OPC remains a complex enterprise, however, and is bedeviled by the one question that has confronted criminologists when it comes to counting crime throughout history, namely: what is the unit to be counted? Conceptually, OPC may present many fascinating issues, but for counting purposes there is really only one problem – how is one crime distinguished from another? In this regard, counting OPC, whether by offenses, offenders or victims, really requires criminologists to ask the same questions. Criminologists have traditionally counted discrete acts as separate 'crimes,' but have consistently wrestled with the conundrum of how to count criminality which is, in effect, spread out over several acts such as spree or serial/repeat offenses. Of course, the effect of a decision to count a series of offenses as 'one' offense has a radical effect on crime counts. OPC is no different in this regard, though the ability to collect millions of records in a single data breach raise the possibility that the measurement implications are much more dramatic. With offenders operating computer systems that seek continually to hack and subsequently to exploit personal data, it is hard to say when one offense ends and another begins. Stealing credit cards may be one criminal act, but in using them one may commit many more.

When it comes to counting 'the victim' and, relatedly, 'the victimization', the same problem occurs. Clearly, victims are a diverse group and victimizations vary in

their financial impact, but for counting purposes the real challenge is saying where one victim, and one victimization, begins and ends. Recall that in the case of arson, the FBI has given up on calculating losses because it seems unreasonable to attribute the losses from a fire that burns out of control to a single offense. But there is no really logical basis for this decision, except to say that calculating losses in this way would produce wildly disparate estimates of losses occasioned by arson that might in some way distort the appearance of how serious the problem really is. In the same way, OPC victims may experience losses from their experiences that go far beyond the financial. They may suffer personal inconvenience as they try to piece their lives back together, or other collateral financial consequences as credit ratings drop or checks bounce. Arguably one can go much further than this: victims might suffer psychological problems, as may the people around them who experience the trauma vicariously. Even readers of this article may be victims should they experience some increment of anxiety in contemplating the extent of OPC. For counting purposes, then, where does one stop? If one is to count the number of victims or characterize the extent of victimization, one has to draw some limits, even in the knowledge that such limits are necessarily arbitrary.

Finding a way to compute OPC rates of either prevalence or harm in a way that permits them to be 'compared' or 'collated' in some way to figures related to traditional property crime may one day be possible, therefore, but only after a series of decisions has been made on how to define the units of count in ways that are broadly acceptable to the criminological community. The sense in which these figures can indeed be 'collated' meaningfully with existing measures such as the UCR 'index crime' rate, however, will depend heavily not only upon the compatibility of the counting rules with those

employed for traditional crime (about which there will no doubt be considerable debate) but also whether criminologists themselves can be convinced that such a collation is wise.

Stepping back from the conceptual issues that this question elicits, however, one can at least return to the preliminary assertion that underlies this paper: namely that increases in OPC may not only be large enough to merit policy attention but also that they may exist in contrasting relation to trends in traditional property crime. As artefactual as such a relationship may be and as tentative as the suggestion must be, given the state of existing data, one urgent question may be to examine the data further for any such relationship and the mechanisms that might underlie it. Obviously, there are many possible causal relationships between OPC and traditional property crime, including some compatible with the suggestion that their countervailing trends are evidence of some interaction. We can speculate that engrossment in online media may cause criminals to change their methods strategically. Simultaneously, fewer real-world interactions may occur, reducing opportunities for traditional property crime to occur. The theoretical implications of such relationships for our understanding of the crime drop itself may be multi-faceted and certainly warrant further exploration. For example, some direct-contact predatory crimes may turn violent precisely because of the proximity of the offender and victim in time and space. This is not so true for cyber predatory crimes since the two never meet in person. So, one indirect consequence of property crimes occurring online could be a drop in the violent crime rate. Of course, some violent crimes may occur online as would be the case with cyber bullying and sexual predators of minors. But they may also escape the notice of the police. Alternatively, time spent online by most youth

of the peak crime-prone age is seen by some researchers as a self-incapacitation mechanism, leading to the decrease in traditional crimes (Ward, 2011).

In short, available data raise the possibility OPC is a growing problem and that, whether incorporated into index crime measures or not, criminologists would be wise to be circumspect before declaring that crime has dropped as radically as traditional measures appear to reflect. The scope for new measurement techniques to capture OPC is clearly wide, as work in the area has barely begun and definitional questions remain pressing. Most importantly, however, the theoretical implications of incorporating an understanding of OPC into observations of crime trends generally are that criminologists must revisit the fundamental assumptions that have underpinned approaches to measuring crime that stretch back for the entire history of the discipline.

REFERENCES

Addington, L. A. (2010). *Measuring crime: Oxford bibliographies online research guide*. Oxford University Press, USA. Retrieved from http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0057.xml

Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33*, 19–29.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2012). *Measuring the cost of cybercrime.* Paper presented at the11th Annual Workshop on Information Security (WEIS), Berlin, Germany, 25–26 June 2012. Retrieved from http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

Baum, K. (2006). *Identity theft, 2004*. Washington, DC: Bureau of Justice Statistics. Retrieved from http://bjs.gov/content/pub/pdf/it04.pdf

Baumer, E., & Wolff, K. T. (2014). Evaluating contemporary crime drop(s) in America, New York City, and many other places. *Justice Quarterly, 31*(1), 5-38.

Biderman, A. D., & Lynch, J. P. (1991). *Understanding crime incidence statistics: Why the UCR diverges from the NCS*. New York, NY: Springer.

Biderman, A. D., & Reiss, A. J. (1967). On exploring the" dark figure" of crime. *The Annals of the American Academy of Political and Social Science*, *374*(1), 1–15.

Blumstein, A., & Wallman, J. (2005). *The crime drop in America.* New York: Cambridge University Press.

Bureau of Justice Statistics (2006). *Data collection: National computer security survey (NCSS).* Retrieved from http://bjs.ojp.usdoj.gov/index.cfm?ty=dcdetail&iid=260

Cheney, J. S. (2003). *Identity theft: A pernicious and costly fraud.* FRB of Philadelphia Payment Cards Center Discussion Paper. Philadelphia: Federal Reserve Bank of Philadelphia. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=927415

Cheney, J. (2005). *Identity theft: Do definitions still matter?* FRB of Philadelphia Payment Cards Center Discussion Paper. Philadelphia: Federal Reserve Bank of Philadelphia. Retrieved from http://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2005/identity-theft-definitions.pdf

Clarke, R., & Newman, G. (2002). *Modifying hot products.* London: Home Office.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44,* 588–608.

Copes, H., & Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy, 8*, 237–262.

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, *38*(5), 1045–1052.

Curtis, R. (1998). The important transformation of inner-city neighborhoods: crime, violence, drugs, and youth in the 1990s. *Journal of Criminal Law & Criminology, 88* (4), 1233-76.

Davies, A. (2012). "Claiming Victim Identity: A Social-Psychological Analysis" in Morosawa, H., Dussich, J. J. P. and Kirchhoff, G. F. (eds.), *Victimology and Human Security: New Horizons*, Nijmegen (NL): Wolf Legal Publishers.

Elbirt, A. J. (2005). Who are you? How to protect against identity theft. *Technology and Society Magazine, IEEE*, *24*(2), 5–8.

Finklea, K. M. (2012). *Identity theft: Trends and issues*. Congressional Research Service. Retrieved from http://www.fas.org/sgp/crs/misc/R40599.pdf

Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. In *Economics of Information Security and Privacy III* (pp. 35–53). New York: Springer. Retrieved from http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf

Goldberger, A., & Rosenfeld, R. (Eds.). (2008). *Understanding crime trends: Workshop report.* Washington, DC: National Academies Press. Retrieved from http://www.nap.edu/catalog/12472.html

Gordon, G. R., Rebovich, D. J., Choo, K., & Gordon, J. B. (2007). *Identity fraud trends and patterns: Building a data-based foundation for proactive enforcement*. Utica College Center for Identity Management and Information Protection, U.S. Department of Homeland Security, Secret Service. Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf

Harlow, C. W. (1985) *Reporting Crimes to the Police*. Special report, #NCJ-99423. Washington DC: Bureau of Justice Statistics.

Harrell, E. and L. Langton. (2013). *Victims of Identity Theft, 2012*. Bulletin #NCJ-243779. Washington DC: Bureau of Justice Statistics.

Hart, T. C. and C. Rennison. *Reporting Crime to the Policy, 1992-2000.* Special report, #NCJ-195710. Washington DC: Bureau of Justice Statistics.

House of Lords Science and Technology Committee (2007). *Personal internet security, 5th report of 2006–07.* London: The Stationery Office. Retrieved from http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Huff, R., Desilets, C., & Kane, J. (2010). *The 2010 national public survey on white collar crime.* Fairmont, WV: National White Collar Crime Center. Retrieved from http://www.nw3c.org/docs/publications/2010-national-public-survey-on-white-collar-crime.pdf?sfvrsn=8

Internet Crime Complaint Center (2013). *2013 internet crime report.* Retrieved from http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

Javelin Strategy & Research (2009). *2009 Identity Survey Fraud Report: Consumer Version*. Pleasanton, CA: Javelin.

Javelin Strategy & Research (2011). *2011 identity fraud survey report: Consumer version.* Available from https://www.javelinstrategy.com/

Javelin Strategy & Research (2012). *2012 identity fraud survey report: Consumer version.* Available from https://www.javelinstrategy.com/

Langton, L. (2011). *Identity theft reported by households, 2005–2010*. Washington, DC: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2207

Langton, L. and Planty, M. (2010). *Victims of identity theft, 2008.* Washington, DC: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/index.cfm?ty=pbdetail&iid=2222

Levitt, S. D. (2004). Understanding Why Crime Fell in the 1990s: Four Factors that Explain the Decline and Six that Do Not. *The Journal of Economic Perspectives*, *18*(1), 163-190.

Loftin, C., & McDowall, D. (2010). The use of official records to measure crime and delinquency. *Journal of Quantitative Criminology*, *26*(4), 527–532.

Lynch, J. P. and Addington, L. A. (Eds.). (2007). *Understanding crime statistics: Revisiting the divergence of the NCVS and UCR*. New York, NY: Cambridge University Press.

Melbin, M. (1978). Night as frontier. *American Sociological Review, 43*(1), 3–22.

Milne, G. R. (2003). How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs, 37*, 388–402.

Mishra, S., & Lalumière, M. L. (2009). Is the crime drop of the 1990s in Canada and the USA associated with a general decline in risky and health-related behaviors? *Social Science and Medicine, 68*, 39–48.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*(3), 3–20.

Morris, R. G. (2010). Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995–2005. *Deviant Behavior*, *31*(2), 184–207.

Mosher, C. J., Miethe, T. D., & Phillips, D. M. (2002). *The mismeasure of crime*. Thousand Oaks, CA: Sage Publications.

National Conference of State Legislatures (2014). *Security Breach Notification Laws.* Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Newman, G. R. (2003). *Check and card fraud*. U.S. Department of Justice, Office of Community Oriented Policing Services. Retrieved from http://www.popcenter.org/problems/pdfs/check_and_card_fraud.pdf

Newman, G. R. (2009a). Cybercrime. In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.), (2009). *Handbook on crime and deviance* (551–584). New York, NY: Springer.

Newman, G. R. (2009b). Policy thoughts on "bounded rationality of identity thieves." *Criminology & Public Policy, 8*, 271–278.

Open Security Foundation. (n.d.). *DataLossDB project.* Retrieved from: www.datalossdb.org

Pew Research Center (2013). *Internet and American Life Project*. Retrieved from http://www.pewinternet.org/

Piquero, N., Cohen, M., & Piquero, A. (2011). How much Is the public willing to pay to be protected from identity theft? *Justice Quarterly, 28*(3), 437–459.

Ponemon Institute (2012). *2012 Cost of cyber crime study: United States. Ponemon Institute Research Report.* Retrieved from: http://www.ponemon.org/library

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and Internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*, 267–296.

Rantala, R. R. (2008). *Cybercrime against businesses, 2005*. Washington, DC: Bureau of Justice Statistics. Retrieved from: http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management, 30*(2), 256–286.

Savitz, L. D. (1978). Official police statistics and their limitations. *Crime in society*, 69–81.

Skogan, W. G. (1977). Dimensions of the dark figure of unreported crime. *Crime & Delinquency*, *23*(1), 41–50.

Skogan, W. G. (1984). Reporting crimes to the police: The status of world research. *Journal of Research in Crime and Delinquency*, *21*(2), 113–137.

Smith, R. G. (1999). Organisations as victims of fraud and how they deal with it. *Trends and issues in crime and criminal justice, Vol. 127*. Canberra, Australia: Australian Institute of Criminology.

Sullivan, R. J. (2010). The changing nature of US card payment fraud: Industry and public policy options. *Federal Reserve Bank of Kansas City, Economic review, Second quarter*, 101–133.

Symantec (2011). *Symantec internet security threat report: Trends for 2010, Vol. 16.* Retrieved from: http://www.symantec.com/threatreport/

Symantec (2012). *Symantec internet security threat report: 2011 Trends, Vol. 17.* Retrieved from: http://www.symantec.com/threatreport/

Taylor, N. (2002). Reporting of crime against small retail businesses. *Trends and issues in crime and criminal justice, Vol. 127.* Canberra, Australia: Australian Institute of Criminology.

Truman, J. (2011). *Criminal victimization, 2010. Bureau of Justice Statistics Bulletin.* Washington DC: Bureau of Justice Statistics. Retrieved from http://bjs.ojp.usdoj.gov/content/pub/pdf/cv10.pdf

Tseloni, A., Mailley, J., Farrell, G. & Tilley, N. (2010). Exploring the international decline in crime rates. *European Journal of Criminology, 7*(5), 375–394.

U.S. Department of Justice. (2013). *Identity theft and identity fraud*. Retrieved from http://www.justice.gov/criminal/fraud/websites/idtheft.html

U.S. Federal Bureau of Investigation. (2013). *Crime in the United States, 2001–2012*. United States Department of Justice. Retrieved from http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/

U.S. Federal Trade Commission. (2004). *National and state trends in fraud & identity theft, January–December 2003.* Retrieved from http://www.ftc.gov/os/2003/09/synovatereport.pdf

U.S. Federal Trade Commission. (2008). *Consumer fraud and identity theft complaint data, January–December 2007.* Retrieved from http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

U.S. Federal Trade Commission. (2011). *Consumer sentinel network data book for January–December 2010.* Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

U.S. Federal Trade Commission. (2012). *Consumer sentinel network data book for January–December 2011.* Retrieved from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2011.pdf

Wadsworth, T. (2010). Is immigration responsible for the crime drop? An assessment of the influence of immigration on changes in violent crime between 1990 and 2000. *Social Science Quarterly*, *91* (2), 531-553.

Ward, M. R. (2011). Video games and crime. *Contemporary Economic Policy*, *29*(2), 261–273.

White, M. D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review*, *19*(1), 3–24.

Xie, M., Pogarsky, G., Lynch, J. P., & McDowall, D. (2006). Prior police contact and subsequent victim reporting: Results from the NCVS. *Justice Quarterly*, *23*(4), 481–501.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407–427.

Zawitz, M.W., Klaus, P.A., Bachman, R., Bastian, L.D., DeBerry, M.M., Rand, M.R. & Taylor, B.M. (1993). *Highlights from 20 Years of surveying crime victims. The National Crime Victimization Survey, 1973–92,* Bureau of Justice Statistics Special

Report NCJ-144525. Washington DC: U.S. Government Printing Office. Retrieved from https://www.ncjrs.gov/pdffiles1/bjs/144525.pdf

Zimring, F. E. (2006). *The great American crime decline.* New York: Oxford University Press.

Table 1. National Estimates of Incidence/Prevalence of Identity Theft and Traditional Property Crime

	Javelin, identity theft/fraud victimizations	**UCR, all property crime reported to police**	**NCVS, identity theft victimizations**	**NCVS, property crime victimizations**
Year	**% adults affected**	**rate per 100 population**	**% households affected**	**rate per 100 population aged 12+**
2003	4.7	3.6	-	16.3
2004	4.3	3.5	3.1	16.1
2005	4.0	3.4	5.5	15.4
2006	3.7	3.3	-	*16.1***
2007	3.6	3.3	6.6	14.7
2008	4.3	3.2	5.0*	13.5
2009	4.8	3.0	7.3	12.7
2010	3.5	2.9	7.0	12.0

* refers to individuals, not households (a different method was employed)
** data for 2006 NCVS were gathered using a different methodology and should be interpreted as a part of the series with caution

Sources of data: Javelin Strategy & Research; Uniform Crime Reports (Crime in the United States); National Crime Victimization Survey

Table 2. Percent of Victims Who Notified Police or Contacted Law Enforcement to Report Victimization

	FTC (identity theft)		NCVS (property crime)	NCVS (identity theft)	NW3C survey (identity theft and credit card fraud)
	notified police	**report taken by police**	**reported to police**	**contacted law enforcement**	**reported to a crime control agency**
2001	49%	40%	37%	-	-
2002	45%	36%	40%	-	-
2003	40%	31%	38%	-	-
2004	39%	30%	39%	-	-
2005	40%	30%	40%	-	20%
2006	38%	30%	38%	-	-
2007	35%	27%	37%	-	-
2008	36%	28%	40%	17%	-
2009	(73%)	(62%)	39%	-	-
2010	(72%)	(62%)	39%	-	26%
2011	(70%)	(57%)	37%	-	-

Note: Data in parentheses should be interpreted with caution since they are based on the information gathered from less than half of the ID theft victims who contacted the FTC directly (the rest of the victims did not provide information about law enforcement contact). For example, 81% of victims provided this information in 2008 but only 42% of victims did so in 2009 and subsequent years.

Sources of data: FTC (2004, 2008, 2012); NCVS (2001–2011); Copes et al. (2010); Huff et al. (2010).

Table 3. National Estimates of Monetary Losses from Online and Traditional Property Crime

	Javelin, identity theft/fraud victimizations	**UCR, all property crime reported to police**		**NCVS, identity theft victimizations**	**NCVS, property crime victimizations**
Year	**monetary loss, in billion $**	**monetary loss, in billion $**	**monetary loss doubled***	**monetary loss, in billion $**	**monetary loss, in billion $**
2003	$58	$17.0	$34.0	-	$14.4
2004	$60	$16.1	$32.2	-	$14.7
2005	$57	$16.5	$33.0	$10.4	$15.6
2006	$50	$17.6	$35.2	-	*$16.5***
2007	$45	$17.6	$35.2	$14.5	$16.1
2008	$48	$17.2	$34.4	$16.6**	$16.2
2009	$54	$15.2	$30.4	$13.3	-

* to adjust for non-reporting using a conservative approach
** direct losses only
*** data for 2006 NCVS were gathered using a different methodology, should be interpreted as a part of the series with caution

Sources of data: Javelin Strategy & Research; Uniform Crime Reports (Crime in the United States); National Crime Victimization Survey

Table 4. Twelve Largest Domestic Incidents of Security Breaches Officially Reported in the U.S. in 2005–2014, Resulting in Losses of Customers' Personal and Financial Data

Number of records exposed	Type of information stolen	Method of data security breach	Date	Organization
152,000,000	Customers' names and IDs, encrypted credit card numbers and passwords	Hack	2013-10-03	Adobe Systems, Inc.
145,000,000	Customers' names, email addresses, personal addresses and phone numbers, DOB	Hack	2014-05-21	eBay Inc.
130,000,000	Credit card numbers	Hack	2009-01-20	Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank
110,000,000	Customers' names, addresses, phone numbers, and credit card info	Hack	2013-12-18	Target Brands, Inc., Fazio Mechanical Services, Inc.
94,000,000	Credit card numbers	Hack	2007-01-17	TJX Companies Inc.
77,000,000	Personal info, possibly credit card info	Hack	2011-04-26	Sony Corporation
40,000,000	Credit card numbers	Hack	2005-06-19	CardSystems, Visa, MasterCard, American Express
35,000,000	Account info, personal info, encrypted credit card numbers	Hack	2011-11-10	Steam (Valve, Inc.)
32,000,000	Account info (user names and passwords)	Hack	2009-12-14	RockYou Inc.
26,500,000	Personal info (name, SSN, DOB) of U.S. military veterans	Stolen computer	2006-05-22	U.S. Department of Veterans Affairs
24,600,000	Personal info, bank account info, credit card numbers	Hack	2011-05-02	Sony Online Entertainment, Sony Corporation
24,000,000	Personal info, account info	Hack	2012-01-15	Zappos

Source of data: Open Security Foundation (www.DataLossDB.org)