Exploring the possibility of ‘moral hazard’ among victims of identity fraud. The relation between reimbursement for unauthorized cash withdrawals and risky online behavior

Johan van Wilsem[1]

Due to digitalization of modern societies, identity fraud is becoming a serious problem. Until recently, Dutch victims of unauthorized cash withdrawals from their bank accounts were reimbursed by their banks in most instances. Because most victims were not confronted with financial damages, this generous reimbursement policy may have unintendedly stimulated moral hazard among victims, due to a lack of incentives to change risky behavior and avoid future victimization. This chapter therefore compares post-victimization changes in Internet activities among reimbursed victims of identity fraud and non-reimbursed victims, as well as non-victims. For this purpose, large-scale, representative longitudinal data were used from the Dutch LISS-panel. Overall, we found no differences in Internet activity change between the distinguished groups. Significant differences were found for shifts in PC security measures, with steepest increases in protection for reimbursed victims. Overall, this points to the absence of moral hazard in this specific case.

1 Introduction

Currently, identity fraud seems to be one of the fastest growing crime types (Benson, 2009), and therefore it is a topic of clear concern. Alongside this increase goes the digitalization of many public and commercial services. Nowadays, client-organization interactions often involve authentication procedures that require online use of personal identification information, such as usernames, passwords, credit card numbers, social security numbers, et cetera (NCSC, 2014). The criminal misuse of such procedures first involves identity *theft*, which is the illegal capture of such identifying information. In the current digital age, this is oftentimes possible by hacking operations. A subsequent step is identity *fraud*, which is the act of using this information by pretending to be someone else (e.g. using someone else’s username and password or credit card information), and performing a financial transaction with it on behalf of the victim’s identity. Companies and government services that use (digital) authentication procedures have databases including these personal identifiers, and the increasing use of such procedures leads to a growth of client databases (Bijlsma et al., 2014).

[1] Johan van Wilsem is an Associate Professor of Criminology at Leiden University, the Netherlands.

According to Schermer and Wagemans (2009), the average citizen in the Netherlands is registered in hundreds of databases. These databases are nowadays 'hot products' (Clarke, 1999) for hackers, because successful breaches of such data, involve the theft of thousands or millions of people's identifying information that can deliver considerable profit to sellers. The Darkweb, a hidden part of the Internet that provides anonymity through encryption of digital user traces, hosts marketplaces for trade in bulks of credit card details and malware that can facilitate ID-fraud operations (Holt & Lampke, 2010).

Another major development relevant to the development of identity fraud as an increasingly relevant crime phenomenon, is the growth of social media use, for instance on Facebook, Twitter, Linkedin, et cetera. In 2015, usage of social media among adults was estimated at 65%, with notably higher rates among young adults, totaling up to 90% (Pew Research Center, 2015).The information on social networking sites enables hackers to construct profiles of users and provide potential for abuse (Nosko et al., 2010). In addition, Acquisti and Gross (2009) showed that with publicly available data on social networking sites (e.g. place and date of birth), social security numbers can be predicted to quite some extent, thereby contributing to the risk of identity fraud.

Therefore, the contemporary social context is one in which identity fraud is a large and costly societal problem. Nevertheless, reliable estimates on the volume of this problem are scarce, as the number of studies on the prevalence of identity fraud using representative samples is limited. Nonetheless, in the US, UK, Australia and the Netherlands, examples of such studies exist, showing annual estimates of approximately five to ten percent of the general population aged 15 years and older (Domenie et al., 2013; Harrell & Langton, 2013; Smith & Hutchings, 2014; UK National Fraud Authority, 2012). However, one of the difficulties in measuring (and comparing) volume estimates lies in the different question wording on identity fraud as well as sampling procedures. Despite these differences, the estimates make clear that identity fraud hits a considerable number of people, and is a major cause of financial damage. In the US, the estimate for 2014 from the Bureau of Justice Statistics was that in total, victims lost over 15 billion dollars over identity fraud incidents (Harrell, 2015).

In an incident of identity fraud, the initial financial damage is borne by the individual client. After that, reimbursement is often possible. In the Netherlands, a representative survey in 2010 uncovered that an estimated 80% of the victims of banking fraud were reimbursed, most of the time for the total amount (Van Wilsem et al., 2013). However, compensation schemes to victims sometimes have an unintended negative side-effect, known as moral hazard. The general mechanism behind it entails that protection of one kind may lead to a decrease of other precautionary measures or the increase of risky behaviors, because the protection leads to a reduction in the perceived chances of harm. Thus, such compensation schemes may offer perverse incentives to victims for their future behavior. Eventually, the increase of criminal opportunities offered by this behavioral change sometimes leads to higher chances of crime victimization. Moral hazard has first been named as a possible side-effect of insurance (Shavell, 1979), but may also be applicable to reimbursement cases in identity fraud. To my knowledge, this chapter is the first study to empirically address this issue.

In the field of criminology, several examples can be mentioned as cases of moral hazard (Grabosky, 1996). In general, they make clear that people can show riskier behavior once they are better protected. For example, O'Leary et al. (1985) found that assertiveness training among battered wives may contribute to the escalation of intimate violence. Firearm possession may not only lead to enhanced possibilities for self-protection, but may also contribute to the escalation of violent conflict (Cook, 1983). Humanitarian intervention to prevent ethnic cleansing have sometimes led to more risk seeking of rebellious groups, retaliation and ultimately to more genocidal deaths (Kuperman, 2008). Insurance may lead to more risk seeking and people watching out less carefully after their belongings (Heimer, 1985). In cases of identity fraud, a similar mechanism may occur: once victims are reimbursed for the financial losses, there is less incentive to alter behavior in a way that prevents future victimization, considering the lack of financial consequences that go along with it. Therefore, in case of a friendly reimbursement regime, moral hazard among identity fraud victims is a possibility. The empirical question therefore is whether (lack of) change in risk-enhancing activities, such as online banking and online shopping, is related to receiving reimbursement.

In this chapter, I therefore compare the changes in online behavior between reimbursed and non-reimbursed victims of identity fraud in the Netherlands. I will do so for the period 2010-2012, in which there was a generous banking regime, with approximately 85% of victims receiving reimbursement (Van Wilsem et al., 2013). For both years, I will examine patterns of change before and after victimization: did someone perform an Internet activity more or less? Besides risk-enhancing behavior, changes in computer security are also scrutinized, such as having a firewall. That way, it is possible to detect whether victims are more likely to install PC security measures if they did not receive reimbursement after identity fraud. Using longitudinal data to address dynamics in computer use and factors responsible for those movements is a novelty to cybercrime victimization research. However, such data are highly needed in order to answer research questions that have a dynamic component (Holt & Bossler, 2014), as is the case here.

As a baseline, non-victims are also included in the comparison. That way, it is possible to see if victims of identity fraud show different patterns of behavioral change, regardless of whether or not one is reimbursed. As victimization is a negative event, behavioral change may be directed towards preventing future victimization, and therefore lead to reduced exposure to offenders by reducing time spent on the Internet. On the other hand, victimization may also induce strain among those that experience it, leaving maladaptive coping to be a possibility. In that case, victimization is disrupting to a degree that certain behavioral adaptations –such as anger and substance abuse– lead to *more* victimization risk (Turanovic & Pratt, 2014).

Apart from whether or not victims were reimbursed, online behavioral change may also depend upon other event characteristics of the identity fraud that define its seriousness. More specifically, victims may have faced a more serious case of identity fraud the higher the amount of money lost. Also, incidents that were reported to the police may also indicate a more serious event. Thus, in order to allow for alternative explanations for shifts in online behavioral patterns, I also address these event characteristics. Furthermore, shifts in Internet activities may partly result from personal characteristics. On that level, low self-control has been argued to be responsible for consistency or even increase in risk-seeking behavior across time (Turanovic & Pratt, 2014). In addition, Reisig et al. (2009) showed that despite the fact that impulsive people perceive more online risks, they do not act accordingly, considering their higher engagement in online purchasing. For the current research problem, though Dutch banks are granting reimbursement most of the time, they may see grounds to deny it based on careless behavior of clients (Van der Meulen, 2011). Such careless or impulsive behavior seems more likely among individuals with low self-control. Therefore, in order to disentangle the relations between reimbursement, online behavioral change and other potentially confounded factors, this research adjusts for individuals' level of self-control.

Data

The data used for this research are drawn from a large, longitudinal Dutch survey, the LISS panel. The sample for this panel is drawn by Statistics Netherlands and is representative for Dutch households. The panel only includes Dutch-speaking, non-institutionalized people aged 15 years or older. The Dutch research organization CentERdata was responsible for data collection, which occurred via an online questionnaire. Respondents in this panel answer questions on a monthly basis, on a variety of topics, such as health, personality and labor. For this, they receive a small financial incentive. In February 2010 and 2012, they answered questions on identity fraud victimization involving unauthorized cash withdrawals from their banking account. Also, they responded to questions on online routine activities and pc security behavior. As they were answered for two waves, it was possible to detect patterns of *change*, and to use the victimization event -and the possible reimbursement- as an event in between. In 2010, 5,376 participated in the panel; in 2012, this number was 5,709.[2] In total 4,042 respondents participated in both the 2010 and the 2012 wave.

[2] In between these years, there was some replacement of the panel. Also, respondents have a choice each month to participate or not. This explains some of the changes in panel size between the two years.

Operationalizations

Victimization, reimbursement and other incident characteristics. In order to establish ID-fraud victimization incidents that occurred between 2010 and 2012, I used the retrospective data from the 2012 wave. During that interview, respondents were asked whether an amount of cash was withdrawn from their banking account without their permission, during the past two years. Therefore, the question applied to incidents that occurred in the period February 2010-February 2012. Of all respondents that participated in both the 2010 and 2012 wave and that gave a valid answer to this question (N=3,959), 3.4% indicated that they had experienced such an incident at least once (N=134). In order to establish the initial financial damage, victims were asked how much money was withdrawn from their account. After that, they were asked if they succeeded in getting their money back through a reimbursement, on which 92% of victims gave a valid answer (N=123). Response categories to this were: (1) *'yes, fully reimbursed'*, (2) *'yes but only partly'* and (3) *'no'*. Based on this, two groups of victims were distinguished: those that got full reimbursement (N=100) and those that did not (N=23).[3] In addition, a group of non-victims was identified (N=3,748).

As a proxy measure of seriousness of the offence, respondents were asked how much money was initially lost in the incident. In order to prevent some outliers with exceptionally high losses to have a disproportionate influence on the results, a cap value was set at 2,500 euros[4] for cases that went over that amount.[5] The average initial amount of money lost was somewhat higher for the reimbursed group – with a median of 170 euros compared to 60 euros for the non-reimbursed – but the difference was not significant.[6] Finally, as a final proxy measure for seriousness of the offence, we asked victims whether they reported the incident to the police (yes/no).

Internet activities and security behavior. In order to measure unintended exposure to Internet offenders, respondents were asked to indicate the amount of time spent in an average week to several online activities. The following activities were included for this: buying products online, online banking, chatting and visiting Internet forums. The same questions were asked in the 2010 and 2012 wave. By subtracting the number of hours between these two years, changes in online activities was established.[7] Thus, negative values indicate a reduction in time spent to an activity, while positive values indicate an increase. Besides this, changes in webcam use were also measured by differencing

[3] Almost anyone in this group received no reimbursement whatsoever.
[4] One euro is worth approximately 1.10 US dollars (March 4, 2016).
[5] For cases with missing values, the median value (100 euros) was inserted. Non-victims scored 0 euros on this indicator.
[6] According to a Mann-Whitney test, a non-parametric test that compares mean rank scores between two groups. Considering the existence of outliers on financial damage, with some single observations reporting much damage, this analytic procedure was preferred over a regular T-test.
[7] For a few respondents, outlier values on the number of hours per week devoted to a certain activity were recoded to values at the 99th percentile, in order to ensure that general patterns were not distorted by extreme values.

the dichotomous answers (0: no – 1: yes) for the two years. In addition, respondents were asked if they had a personal profile on social networking sites. For both years, this was asked for thirteen different sites, such as Facebook, MySpace and the Dutch site Hyves. Positive answers were summed into a scale to indicate online visibility through social network membership.

With regards to PC security measures, for both waves I used data on whether or not (0-1) respondents, to their knowledge had installed (a) a firewall, (b) a virus scanner, (c) antispy software, (d) a Trojan scanner, (e) a spam filter and/or (f) wireless network security measures. For this, the items were summed in order to estimate the amount of PC prevention activities they had undertaken, in 2010 and in 2012. The difference between these sums reflect changes in PC security actions across time.

Low self-control. Previous studies have used various ways to measure low self-control, for instance by focusing on immediate gratification (impatience), impulsiveness, *or* antisocial propensity (e.g. Holtfreter et al., 2008; Pratt and Cullen, 2000). In this study, low self-control is measured by twelve items of dysfunctional impulsivity from the Dickman Impulsivity Inventory (Dickman, 1990), which assesses self-reported difficulty with the regulation of behavioral impulses. Each item refers to a trait that the respondent has to indicate whether they agree (no=1/yes=2) that they are like that (e.g. 'I often say and do things without considering the consequences'; 'I frequently buy things without thinking about whether or not I can really afford them'). For scale construction, the mean value was computed for the twelve dichotomous responses in the 2010 wave (Cronbach's α = 0.73). From the sample, 43 percent indicated no signs of low self-control for all items. Approximately 4 percent of all respondents reported poorly controlled behavior on at least half of the items.

Descriptives

Table 1 shows an overview of the descriptives of the variables used in this research. Regarding the overall dynamics in computer use, the results from this table are insightful for a couple of reasons. First, they show that, on average, several online activities were performed at a greater intensity at T2 (2012) compared to T1 (2010). These are online shopping, online banking, the number of profiles on social networking sites, and webcam use. Comparing the means between the two years also reveals that these increases are not dramatic, but rather point to slight acceleration. Second, there also online activities that, on average, follow a countertrend: they were slowed down somewhat among this group of respondents. This holds for chatting and Internet forum use. Finally, the number of PC security measures proved to be quite constant across the two time points, at almost three measures taken on average.

Table 1 about here

Analysis

For this chapter, analyses are presented in two steps. First, changes between 2010 and 2012 in risk enhancing online activities –for identity fraud victimization- are compared between three groups: (1) victims that were fully reimbursed, (2) victims that were either not fully reimbursed or not at all, and (3) non-victims. This comparison is also done for changes in PC prevention measures. As most variables on change show a skewed distribution and in some cases outliers, non-parametric Kruskall Wallis tests were used to establish significance of differences between the three groups. This test ranks the change levels and compares these ranks, instead of their real values (as in parametric tests such as ANOVA).

Second, linear regression models are used to predict changes in online activities and PC security measures between 2010 and 2012. They model behavioral change as a function of characteristics of the identity fraud incident (reimbursement, police reporting, initial amount of money lost) and respondent characteristics (gender, age, low self-control). Outlier analysis are done by establishing Cook's D levels in each analysis; none of the analysis presented severe outlier problems, with Cook's D values all below 0.25.

3 Results

First of all, shifts in online behavior are examined between the three groups distinguished here: reimbursed victims of ID-fraud, victims that were denied reimbursement, and non-victims. Behaviors considered in this analysis are profiles on social networking sites, online banking, online shopping, chatting, forum use and webcam use. The results in Table 2 make clear that although there are some slight differences between the groups, none of them were significant. Possibly, this partly has to do with the small sample size of the group of victims who did not receive full reimbursement (N=20). Nonetheless, between the larger groups of reimbursed victims and non-victims, no significant differences were found either. An alternative picture emerges for PC security measures, where significant differences in average change patterns were found: reimbursed victims of ID fraud increase the number of prevention measures taken, non-victims stay more or less the same, while non-reimbursed victims tend to downsize their prevention efforts somewhat. Therefore, these findings run counter toward a moral hazard perspective.

Table 2 about here

To shed light on the relation between incident characteristics, individual characteristics and online behavioral change, regression analysis were conducted on the longitudinal data. In these analyses, in order to explain the behavior at Time 2 (2012), the regression equation keeps constant for levels of that same behavior at Time 1 (2010). As such, the regression becomes an analysis of *change*, a regular procedure in panel analysis (Allison, 1990).

Apart from accounting for which group an individual belongs to (reimbursed, non-reimbursed, non-victim), the regression also controls for initial amount of money lost[8], and if the incident was reported to the police. At the individual level, the analysis controls for gender, age and low self-control.

Table 3 about here

The results in Table 3 make clear once again that reimbursement does not seem to play a role in choices to alter online behavior between the years 2010-2012. No significant differences were found between reimbursed and non-reimbursed victims. For several online activities, the single characteristic affecting them is age. For four activities, older people tended to have a smaller increase (and sometimes even a decrease) in the time spent on it. For webcams, there was a development counter to that, with older people showing larger increase in use compared to younger people.

Finally, for PC prevention measures, more significant relations were found. First of all, similar to the bivariate relations in Table 2, the regression results again show that prevention behavior is decreased among those that did not receive reimbursement after ID fraud victimization and among non-victims, compared to reimbursed victims. Therefore, this analysis provides a more robust test, indicating that non-reimbursement's effect on prevention behavior is independent of other incident seriousness indicators and levels of self-control. The latter has its own relation to PC security behavior: the lower the self-control, the greater the chances that prevention efforts are cut back. For women and older people, I also find significantly decreases in prevention between 2010 and 2012, compared to the increases among males and youngsters.

[8] Because of a very few extreme observations, a cap value was defined at 2,500 euros; furthermore, non-victims were assigned 0 (no money lost)

Conclusion

Identity fraud is a crime in the spotlight nowadays. The increasing attention for it has a lot to do with its changing nature and volume, that develops strongly due to the possibilities to commit this kind of fraud in online ways. Increasingly, organizations tend to file their client data in databanks which are targeted by hackers. Also, people tend to share person information in social networking sites; by combining items out of these, personal profiles can be compiled that allow for identity switches in client interaction.

In practice, Dutch victims of identity fraud by unauthorized cash withdrawals mostly receive reimbursement by their bank in order to make up for financial losses. A study on data from 2010 estimate that in 85% of the cases, victims receive such a reimbursement (Van Wilsem et al., 2013). In such a generous regime, moral hazard may have large-scale negative consequences, in which compensated victims unintendedly keep showing risky behavior on the Internet due to a lack of incentives to change online behavior, thereby prolonging future risk of identity fraud victimization.

However, the current results offered little support for this hypothesis. Generally, I found little difference in shifts for five separate online activities between victims with or without reimbursement. Even compared with non-victims, no significant differences were found. For PC security measures, reimbursed victims of ID fraud showed the highest *increase* in prevention behavior, and non-reimbursed victims showing the least increase. Thus, this finding runs counter to a moral hazard perspective, which would expect reimbursed victims to become ‘sloppy’ in their security behavior. These differences remained after controlling for several incident and respondent characteristics, such as reporting the fraud to the police and low self-control. The question therefore is why lack of reimbursement leads to fewer precautionary measures taken. For the moment, two alternative explanations are suggested. First, the denial of reimbursement may frustrate victims and possibly even lead to self-labeling (Grabosky, 1996), which in turn leads to coping mechanisms that deteriorate protection. Second, non-reimbursement may be connected to individual characteristics (e.g. personality that encourage investment in prevention behavior. Future studies in cybercriminology need to invest more in the determinants of prevention behavior in order to shed more light on this.

Do these results show that the moral hazard hypothesis for reimbursement in ID-fraud is falsified? There are four reasons why that conclusion would be premature. First of all, in most cases, the financial losses of victims are quite small – and perhaps too small to infer behavioral change. Analyses on subgroups whose losses are more substantial may show patterns that are more in line with the moral hazard hypothesis. In addition, despite working with large population samples, group size is small, particularly for non-reimbursed victims (N=20), and therefore hampers the ability to find significant differences in empirical analysis. A solution for this is to combine the current data on 2010-2012 with future editions of the same panel.

Secondly, victims of ID-fraud, either reimbursed or not, may fail to see the connection between their victimization (an unauthorized cash withdrawal from their bank account) and their online behavior. In that sense, this type of victimization is quite abstract, without a clear trace how the offender was able to use personal information to commit the crime. Therefore, change of behavior may be more likely if it is clear to the target that such a shift may help for prevention purposes.

Thirdly, behavioral change may have manifested among the distinguished groups, but in a more nuanced way. Obviously, there seems little difference between the groups in indicators measuring overall exposure to offender through the hours spent on the Internet. But this tells us little about the possible changes in more fine-grained (and hard-to-measure) behaviors, such as clicking on infected links, keeping away from specific sites, or not mentioning specific details in profiles on social networking sites. Survey data may not be well-suited to address such nuanced shifts in behavior as respondents are not likely to adequately remember such details. Log data of computer-sessions may provide a better possibility for this.

Fourth, the current study is about patterns of identity fraud, Internet use and precautionary measures in the Netherlands. Clearly, testing hypothesis in other countries is important in order to reveal the presence or absence of consistent results. However, in order to do right to the substantive problem of online behavioral *change*, this involves the start of longitudinal data collection in the area of cybercrime victimization (and ID-fraud in particular) and online activities. In general victimization studies, longitudinal data have been used scarcely (Averdijk, 2011; Ousey et al., 2008; Turanovic & Pratt, 2014), but in studies on *cybercrime* victimization, it is still a novelty. However, they provide new chances to hypothesis testing on the consequences of events (e.g. victimization) for online perceptions and behavior, by comparing them before and after the event (Holt & Bossler, 2014). In turn, such dynamics in online behavior may have consequences for future victimization, with increases in exposure to offenders by more online activity expected to lead to more risk. The extent to which that is the case is however a key issue for future longitudinal studies.

References

Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *PNAS, 106,* 10975-10980.

Allison, P.D. (1990). Change scores as dependent variables in regression analysis. *Sociological Methodology, 20*, 93-114.

Averdijk, M. (2011). Reciprocal Effects of Victimization and Routine Activities. *Journal of Quantitative Criminology*, *27*, 125-149.

Benson, M.L. (2009). Editorial introduction. Offenders or opportunities: approaches to controlling identity theft. *Criminology & Public Policy, 8*, 231-236.

Bijlsma, M., Straathof, B., & Zwart, G. (2014). *Kiezen voor privacy. Hoe de markt voor persoonsgegevens beter kan*. The Hague: CPB. Retrieved from http://www.cpb.nl/publicatie/kiezen-voor-privacy-hoe-de-markt-voor-persoonsgegevens-beter-kan

Clarke, R.V. (1999). *Hot Products: understanding, anticipating and reducing demand for stolen goods*. London: Home Office. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.551.8913&rep=rep1&type=pdf

Cook, P.J. (1983). The influence of gun availability on violent crime patterns. *Crime and Justice, 4*, 49-89.

Domenie, M.M.L., Leukfeldt, E.R., Wilsem, J.A. van e.a. (2013). *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Den Haag: Boom Lemma Uitgevers.

Grabosky, P. (1996). Unintended Consequences of Crime Prevention. *Crime Prevention Studies, 5*, 25-56.

Harrell, E. (2015). *Victims of identity theft, 2014*. Bureau of Justice Statistics. Retrieved from http://www.bjs.gov/content/pub/pdf/vit14.pdf

Harrell, E. & Langton, L. (2013). Victims of Identity Theft, 2012. *Bureau of Justice Statistics*. Retrieved from http://www.bjs.gov/content/pub/pdf/vit12.pdf

Heimer, C. (1985). *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts*. Berkeley: University of California Press.

Holt, T.J. & Bossler, A.M. (2014) An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*, 20-40.

Holt, T. J. & Lampke, E. (2010). Exploring Stolen Data Markets Online: Products and Market Forces. *Criminal Justice Studies*, 23, 33–50.

Holtfreter, K., Reisig, M. D., & Pratt, T.C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology*, *46*, 189–220.

Kuperman, A.J. (2008). The Moral Hazard of Humanitarian Intervention: Lessons from the Balkans. *International Studies Quarterly*, *52*, 49-80.

Nationaal Cyber Security Centrum (2014). *Cybersecuritybeeld Nederland 4.* Retrieved from https://www.ncsc.nl/dienstverlening/expertiseadvies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html

Nosko, A., Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of FACEBOOK. Computers in Human Behavior, 26, 406–418.

O'Leary, D. Curly, A., Rosenbaum, A., & Clarke, C. (1985). Assertion training for abused wives: A potentially hazardous treatment. *Journal of Marriage and Family Therapy*, *11*, 319-322.

Ousey, G.S., Wilcox, P.W., & Brummel, S. (2008). De´ja` vu All Over Again: Investigating Temporal Continuity of Adolescent Victimization. *Journal of Quantitative Criminology*, *24*, 307-335.

Pew Research Center (2015). *Social media usage, 2005-2015.* Retrieved from http://www.pewinternet.org/files/2015/10/PI_2015-10-08_Social-Networking-Usage-2005-2015_FINAL.pdf

Pratt, T.C. & Cullen, F.T. (2000). The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. *Criminology*, *38*, 931–964.

Reisig, M.D., Pratt, T.C., & Holtfreter, K. (2009). Perceived risk of Internet theft victimization. Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice & Behavior, 36*, 369-384.

Schermer, B.W., & Wagemans, T. (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*. Den Haag: College Bescherming Persoonsgegevens.

Smith, R.G. & Hutchings, A. (2014). Identity crime and misuse in Australia: Results of the 2013 online survey. *AIC Reports: Research and Public Policy Series.* Australian Government: Australian Institute of Criminology.

UK National Fraud Authority (2012). *Annual Fraud Indicator, March 2012.* Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf

Van der Meulen, N. (2012). Eigen schuld, dikke bult? Aansprakelijkheid bij fraude met internetbankieren. *Informatiebeveiliging, 8,* 7-11.

Wilsem, J. van, Meulen, N. van der & Kunst, M. (2013). Je geld kwijt, en dan? Financiële schade bij slachtoffers van onrechtmatige bankafschrijvingen. *Tijdschrift voor Criminologie, 55*(4), 360-374

Turanovic, J.J., & Pratt, T.C. (2014). "Can't stop, won't stop": Self-control, risky lifestyles, and repeat victimization. *Journal of Quantitative Criminology*, *30*, 26-56.