European Sociological Review VOLUME 29 | NUMBER 2 | 2013 168–178
DOI:10.1093/esr/jcr053, available online at www.esr.oxfordjournals.org
Online publication 24 June 2011


# 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization

Johan van Wilsem

***Abstract:*** Consumer fraud seems to be widespread, yet little research is devoted to understanding why certain social groups are more vulnerable to this type of victimization than others. This article deals with Internet consumer fraud victimization, and uses an explanatory model that combines insights from self-control theory and routine activity theory. The results from large-scale victimization survey data among the Dutch general population ($N = 6{,}201$) reveal that people with low self-control run substantially higher victimization risk, as well as active online shoppers and people participating in online forums. Though a share of the link between low self-control and victimization is indirect—because impulsive people are more involved in risk enhancing online routine activities—a large direct effect remains. This suggests that, within similar situations, people with low self-control respond differently to deceptive online commercial offers.

## Introduction

For private consumers, the Internet has developed into an important channel for product purchase and orientation. In countries with high densities of Internet access, such as the United Kingdom, Germany, and The Netherlands, more than half of the population made online purchases in the past (Bureau of Statistics, 2008). In the United States, online purchases are made by an estimated two-thirds of adults with online access (Horrigan, 2008), with a total sales worth of e-commerce transactions of approximately $259 billion (Forrester Research, 2007). For The Netherlands, this number amounted to a total of approximately €2.8 billion (Weltevreden, 2007).

Although online product sale leads to easier and cheaper access to consumer goods (e.g. Brown and Goolsbee, 2002), there is also a 'dark side' to online shopping because of the potential for fraud victimization. Several sources suggest that a sizable number of people become the victims of online consumer fraud. Using International Crime Victims Survey data, van Dijk, van Kesteren and Smit (2007) document annual online fraud victimization rates of 1–3 per cent for several Western European countries and the United States. Based on the Federal Trade Commission Survey, Anderson (2007) estimates the number of fraud incidents involving online purchases for the United States to be 6.4 million. According to this survey, the median financial loss suffered by victims who said they paid for something they never received was $60. Estimates of financial damage from the Internet Crime Complaint Center (2008) are higher, with victims suffering average losses of $800, but this selection of victims filed an official complaint, which is probably done more often in serious cases. Importantly, in addition to the financial damage, negative e-commerce experiences erode generalized trust in other people and thus have harmful social effects as well (Mutz, 2009).

This article's focus on online purchases which are not delivered is a specific case within the broader area of consumer fraud. Other examples of consumer fraud include advance fee fraud (e.g. for credit cards), prize promotion fraud (paying for prizes which are never received), and pyramid scheme fraud (Anderson, 2004, 2007). Furthermore, within the field of Internet consumer fraud, other types exist as well. An example is that purchased goods are delivered but that they do not live

Department of Criminal Law and Criminology, Leiden University, PO Box 9520, 2300 RA Leiden, The Netherlands. Email: j.a.van.wilsem@law.leidenuniv.nl

 Submitted: October 2010; revised: May 2011; accepted: May 2011.

up to product descriptions, for instance because of damage. Focusing on the Internet for consumer fraud is becoming increasingly important because it offers an easy way for offenders to contact a large pool of potential victims. As a result, fraud perpetrators are increasingly using online environments in search of suitable targets (Newman and Clarke, 2003). Recent United States and Dutch studies of general consumer fraud estimated that one-fifth to a quarter of all fraud victimizations were initiated via the Internet or e-mail (Anderson, 2007; Oudejans and Vis, 2008). Internet auctions (e.g. eBay, the Dutch marktplaats.nl) are well-known 'places' where online consumer fraud can occur.

This article has two main goals. First, it will give a *national estimate* of the prevalence rate of online consumer fraud victimization, using victimization survey data. This type of data has the general advantage that volume estimates are not distorted by the willingness to report the crime to official agencies, as respondents are asked to report *all* crimes they experienced. Although some sources have presented such estimates before, most of them are from the United States (Anderson, 2004, 2007). Non-US studies use data from several years ago and might be outdated, considering the fast changes in Internet use in Western countries (van Dijk, van Kesteren and Smit, 2007). The current study uses data from 2008 from a representative sample of the Dutch general population in the age group $\geq$16 years ($N = 6{,}201$).

Second, this article sets out to assess *risk factors* for Internet fraud victimization. Compared to other crime types (e.g. violence, burglary), little research is done on risk factors of fraud victimization. Thus, there are few theoretically elaborated attempts to explain why certain groups are more vulnerable than others to consumer deception (Holtfreter, Reisig and Pratt, 2008). Many studies on fraud victimization have focused on demographic profiles (Titus, Heinzelmann and Boyle, 1995; Trahan, Marquart and Mullings, 2005; Anderson, 2006; Holtfreter, Reisig and Blomberg, 2006), and reveal that fraud victims differ in several ways from the young, lower class urban male as the typical victim for street crime. For fraud victimization, higher educated people and high-income households seem to be relatively vulnerable (Titus, Heinzelmann and Boyle, 1995; Anderson, 2006). Furthermore, there are no pronounced gender differences, neither as differences between rural and urban residents. Similar to street crime, youngsters are more often victims of fraud (e.g. Titus, Heinzelmann and Boyle, 1995; Holtfreter, Reisig and Blomberg, 2006).

Relations between socio-demographic characteristics and crime do not reveal *why* people become victims of fraud. In previous research, it has been argued that demographic characteristics are proxy measures for routine activities of everyday life, and—for street crime—that males, youngsters, and urban residents more often fall prey to offenders because they expose themselves and their property by going out at night (Hindelang, Gottfredson and Garofalo, 1978). However, to perform better empirical tests of criminological theories, it is preferable to have direct measures of risk factors (Holtfreter, Reisig and Pratt, 2008). For street crime, several of such tests have been performed (e.g. Mustaine and Tewksbury, 1998), but hardly for fraud victimization. Therefore, this is a primary objective of the present article. Following Holtfreter, Reisig and Pratt's (2008) strategy in their study on consumer fraud, routine activity theory (Cohen and Felson, 1979) and self-control theory (Gottfredson and Hirschi, 1990; Schreck, 1999) are used as leading theoretical approaches, and are applied to Internet consumer fraud victimization. According to routine activity theory, risks of online fraud are concentrated among people who expose themselves to fraudsters by certain online activities—such as purchasing products. Self-control theory argues that people with poor impulse control will more often be defrauded, because they particularly aim for the satisfaction of short-term objectives, and less to the credibility of the offer and potential harmful long-term consequences. Possibly, the two theories are complementary, if people with low self-control are more often fraud victims because they expose themselves to offenders by performing more risky online activities.

This research follows three important recommendations by Holtfreter, van Slyke and Blomberg (2005) to make scientific progress in the field of fraud victimization. First, the use of a nationally representative sample increases the possibilities of generalizability to a larger population, which is quite novel in this field, since 'virtually all previous surveys have been restricted to a single community' (Holtfreter, van Slyke and Blomberg, 2005: p. 267). Second, the inclusion of direct indicators for theoretical concepts improves the potential for testing of hypotheses. Routine activity theory and self-control theory are perspectives that are hardly explored in the context of (online) fraud victimization (Holtfreter, Reisig and Pratt, 2008; Pratt, Holtfreter and Reisig, 2010). Instead, most research in this area has been applied to various types of street crime, such as violence, burglary, and larceny (e.g. Mustaine and Tewksbury, 1998; Schreck, 1999). Third, taking into account that the overwhelming majority of previous

research in this field is from the United States, this article expands the scope of fraud research to the context of The Netherlands and thus offers the potential for international comparison. In this respect, the US study of Holtfreter, Reisig and Pratt (2008) serves as a special case of comparison, since it also focused on the impact of self-control and routine activities on consumer fraud victimization.

## Previous Research

A necessary condition for victimization to occur is that targets (unwillingly) expose themselves to offenders. Thus, the greater this exposure is, the chances of becoming a victim increases, which in turn is related to the target's *visibility* and *accessibility* (Felson and Clarke, 1998).[1] For street crimes, empirical tests of routine activity theory have shown that non-domestic activities, such as going to a bar, elevate victimization risk by bringing targets more often into situations where offenders are also present (Mustaine and Tewksbury, 1998). For online crime victimization, the theory is also applicable (Holt and Bossler, 2009). In general, the Internet is an environment that provides circumstances that assist criminals very well to find suitable targets. With their acronym SCAREM, Newman and Clarke (2003) sum up the reasons for the criminal opportunities on the Internet and their linkage to motivations of potential offenders: *stealth* permitted by aliases, *challenge*, for instance to beat the computing system and manage to trick people into scams despite the security measures in online auctions, the value of *anonymity* for successful crime commission, *reconnaissance* or the easy and cheap opportunity to scan suitable targets and send e-mail scams to a large pool of victims, the possibilities of *escape* to stay out of the hands of legal authorities because it is difficult to link crimes to online perpetrators, and *multiplicity* or the possibility to create new opportunities from a single Internet crime, for instance by hacking information systems or by (online) sharing information on easy-to-persuade victims of consumer fraud. Within such an environment of abundant criminal opportunities, it is assumed that on the Internet, target accessibility and visibility serve as discriminating characteristics to offenders whom they choose to victimize—as they are offline as well.

Target accessibility to Internet fraud offenders is dependent on people's online activities. In this respect, Pratt, Holtfreter and Reisig, (2010) found that Internet fraud targeting (attempted fraud) is more likely among persons who expose themselves to perpetrators by making online purchases and spending time on the Internet. Furthermore, online activities can also result in greater visibility to offenders if a person is actively involved in online forums, if he/she uses a webcam or has personal profiles on social networking sites. Through these activities, a target can unconsciously send out signals of careless behaviour, for instance by revealing much personal details of one's private life. Such information may be used by fraudsters in their decision whom they should target as a victim and how they should approach them in order to gain their trust (social engineering). Summarizing, hypotheses from a routine activity perspective is that people run greater risk to become the victims of online consumer fraud, the more accessible and visible they are to fraud offenders through their online activities.

Self-control theory hypothesizes that people with poor impulse control more often act in the pursuit of self-interest and risk taking, and therefore take decisions with less consideration to their long-term consequences (Gottfredson and Hirschi, 1990). A large body of research has found strong effects of low self-control on *delinquency* and other deviant behaviour, such as gambling, drinking, and traffic accidents (e.g. Forde and Kennedy, 1997; Junger, West and Timman, 2001). Schreck (1999) was the first to extend this perspective to crime *victimization*. He argued that risk taking and lack of preventive behaviour make people more susceptible to this type of event. To date, most empirical support has been found for violent victimization (Stewart, Elifson and Sterk, 2004; Piquero *et al*., 2005; van Wilsem, 2011), while Schreck and his colleagues (Schreck, 1999; Schreck, Stewart and Fischer, 2006) also found supportive results for theft victimization.

In order to explain how low self-control affects online fraud victimization, it is important to understand that consumer fraud is a two-stage process. Consumers are first targeted by fraudsters, and subsequently, some of them are victimized. The choice of fraudsters on who is targeted and who is not seems to take place largely through a process of routine exposure, for instance by contacting those who engage in online shopping (Pratt, Holtfreter and Reisig, 2010). According to Holtfreter, Reisig and Pratt (2008), low self-control plays no role in being targeted or not. They argue that impulsive behaviour is not readily observable to remote (online) offenders and does not serve as an indicator of suitability to offenders during this early stage of the fraud. Indeed, their results show that low self-control has no direct impact on consumer fraud targeting. Simultaneously however, their descriptive results reveal that people with low self-control tend to engage more in remote purchasing, which is their prime determinant of fraud targeting. This finding is in line with Forde and

Kennedy's (1997) hypothesis that people with poor impulse control more often engage in routine activities that lead to increased exposure to offenders. As such, self-control and fraud targeting may be related in an indirect way. This perspective argues that self-control serves as a *selection* mechanism, by structuring which people will be brought into situations that lead to exposure to fraudsters. Indeed, Reisig, Pratt and Holtfreter (2009) offer support for the self-control exposure link with their finding that financially impulsive people made more online purchases than others, even despite the fact they also perceived higher risks of Internet theft.

An alternative possibility is that *given exposure to offenders*, people with low self-control behave in a way that makes victimization more likely to happen. In decisions on buying a product, impulsive people are likely to pay less attention to the supplier's terms of guarantee (Baumeister, 2002), thereby signalling that they are suitable targets to defraud (Holtfreter, Reisig and Pratt, 2008). Instead of selection, this perspective argues that the link between self-control and victimization is one of *causation*. Langenderfer and Shimp (2001) note that scam experts identify low self-control as one of the prime risk factors for fraud victimization. Indeed, Holtfreter, Reisig and Pratt, (2008) find that people with low self-control are more vulnerable to consumer fraud, based on self-reports of victimization from a Florida sample. In addition, they find that self-control is especially risk enhancing among people who are targeted by fraud perpetrators. Once they are targeted, financially impulsive people seem to behave in ways that make them more suitable to defraud, for instance by making risky purchasing choices.

With data on targeting being unavailable, the present article focuses on Internet fraud *victimization*. Low self-control is expected to affect victimization risk in two ways. First, it does so in an indirect way, by determining how much online routine activities one performs that increase exposure to online fraudsters, such as Internet purchasing and forum participation. Second, controlling for the amount of online routine activities, low self-control is also expected to have a direct effect on victimization. Similar to the argument of Holtfreter, Reisig and Pratt (2008), it is expected that self-control's contribution to fraud victimization risk is most pronounced among persons vulnerable to targeting by fraud perpetrators. Therefore, I will test whether low self-control has stronger effects on victimization for people who engage in Internet purchasing, the latter being the prime determinant of Internet fraud targeting (Pratt, Holtfreter and Reisig, 2010).

# Data

This article uses data from the LISS panel, a Dutch large-scale online longitudinal survey, collected by CentERdata in February 2008. Usually, a drawback of online samples is that non-users of computers or the Internet are excluded, resulting in a non-representative sample. For the LISS panel however, respondents were not recruited online, but by telephone or face-to-face, after receiving a recruitment letter.[2] Furthermore, participating households that did not own a pc were given one for the duration of the panel research (~5 per cent of the sample). This procedure resulted in a sample that is by approximation representative for the Dutch population in the age group of ≥16 years.[3] Representativeness is one of the three important advantages of the data used, as some previous studies on fraud victimization have used selective samples, for example among students (Holtfreter *et al.*, 2010) or fraud experts (Langenderfer and Shimp, 2001). Second, the results are based on a *large-scale* data set. It consists of 6,896 respondents from 4,353 households. Since online fraud victimization is the key focus in this article, information is used from 6,373 respondents that indicated they tended to use a computer or the Internet. From this group, 2.5 per cent had missing values on the variables used in the regression analysis. Therefore, the total amount of respondents in the analyses is 6,201. Using such a large sample improves the validity of the estimates of prevalence rates and assessment of risk factors for fraud victimization, because victimization of this kind *during the past year* is a relatively rare event, as is the case for more types of crime. Asking respondents to recall crime events of the most recent year is standard practice in crime victimization research, and yields more valid answers which are less plagued by recall and telescoping bias, compared to recalling events from a longer time ago. Third, the data include *direct indicators* of online routine activities and self-control, offering improved opportunities for hypothesis testing compared to previous fraud research, which often included a demographic comparison between victims and non-victims (Titus, Heinzelmann and Boyle, 1995; Anderson, 2006).

## Measures

*Internet consumer fraud victimization* was established by asking if respondents ever bought a product via the Internet or e-mail, but received no goods. Those who said they did were asked how many times this happened in the past year. I dichotomized this into a measure that distinguishes victims (1) and non-victims (0).

*Low self-control* is measured by using 12 items on dysfunctional impulsivity from the Dickman Impulsivity Inventory (DII) (Dickman, 1990). They assesses self-reported difficulty with the regulation of behavioural impulses, which is hypothesized to be an important source of fraud victimization. Each item refers to behaviour for which the respondent is asked if it adequately describes him or her (yes/no response). For instance: '*I regularly make appointments without thinking if I can live up to them.*' '*I regularly make decisions without considering all aspects of a situation*', and '*I often think too little before I act*'. A continuous scale variable was constructed by computing the mean value for these items ($\alpha = 0.74$). In previous studies, the DII has been used to predict self-reported delinquency (e.g. Heaven, 1993), violent threat victimization (van Wilsem, 2011), Internet addiction (Meerkerk *et al.*, 2010), and academic failure (Vigil-Colet and Morales-Vives, 2005). Caci *et al.* (2003) demonstrated the DII's construct validity.

*Routine Internet activities* are assessed by the average amount of hours per week respondents engage in buying products via Internet or e-mail, and visiting online forums and communities. Dummy variables are constructed if respondents have Internet profiles on Hyves (a popular Dutch social network site), Facebook, or another site, and if they use a webcam. Buying products online is an indicator of a target's accessibility to online fraudsters, while the other Internet activities are indicators of a target's online visibility.

With respect to *demographic characteristics*, respondent's gender, age, and educational level (coded in six categories) are known. For the respondent's household, information is available on whether the household includes two partners (1) or not (0), the household size, the net monthly income, and the degree of urbanization of the residential environment (coded into five categories, ranging from 'not urban' to 'very urban').

Table 1 offers an overview of the descriptives of the variables used in this research.

## Results

Of all respondents, 2.5 per cent indicated they were the victim of Internet consumer fraud during the past year. Bivariate analyses reveal that many victims of online fraud are relatively young. Respondents up to the age of 35 years, more often become victims of this crime (4 per cent), while respondents in the age group ≥55 years face very low risks (~0.5 per cent). No clear differences are found for sex, educational level, and urbanism.

It is hypothesized that people with low self-control may fall prey to consumer deception more often, because of their higher engagement in routine activities that are conducive to fraud (Reisig, Pratt and Holtfreter, 2009). To explore this possibility, self-control is related to several Internet activities (Table 2). Since none of these variables follow a normal distribution, Spearman rank correlations are performed. Indeed, these show that impulsive people are more active on the Internet. Compared to less impulsive people, they spend more hours on average buying products online, visiting Internet forums, and more often they have personal Internet profiles (apart from Facebook). Finally, webcam use is more prevalent among impulsive people.

**Table 1** Descriptives of the dependent and independent variables ($N = 6{,}201$)

| Variables | Mean (SD) | Min. | Max. |
|---|---|---|---|
| Online consumer fraud victimization | 0.02 | 0 | 1 |
| Female | 0.53 | 0 | 1 |
| Age | 45.73 (15.20) | 15 | 94 |
| Educational level | 3.54 (1.50) | 1 | 6 |
| Household size | 3.18 (1.33) | 1 | 9 |
| Household income | 3.18 (12.82) | 0 | 347 |
| Partner present in household | 0.80 | 0 | 1 |
| Degree of urbanism | 3.04 (1.28) | 1 | 5 |
| Internet shopping | 0.40 (0.67) | 0 | 4 |
| Visiting online forums | 0.35 (1.08) | 0 | 7 |
| Social network site: Hyves | 0.27 | 0 | 1 |
| Social network site: Facebook | 0.02 | 0 | 1 |
| Social network site: Other site | 0.04 | 0 | 1 |
| Webcam | 0.16 | 0 | 1 |
| Low self-control | 1.12 (0.16) | 1 | 2 |

**Table 2** Spearman rank correlations between routine Internet activities and low self-control

| Variables | $R_s$ |
|---|---|
| Internet shopping (hours/week) | 0.08** |
| Visiting online forums (hours/week) | 0.09** |
| Internet profile: Hyves (yes/no) | 0.16** |
| Internet profile: Facebook (yes/no) | 0.02 |
| Internet profile: Other (yes/no) | 0.06** |
| Webcam (yes/no) | 0.05** |

*$P < 0.01$

In order to disentangle the determinants of Internet consumer fraud victimization, logistic regression models are estimated (Table 3). In these analyses, the dependent variable is related to self-control, demographic characteristics, and online routine activities.[4] Apart from assessing which factors influence fraud victimization, an additional goal is to examine if low self-control not only has a direct effect but indirect effects as well, via selection into risk enhancing online routine activities. Therefore, in order to evaluate if the effect of self-control on fraud victimization is altered by the inclusion of other indicators, four separate equations are estimated: (i) a bivariate model, including only low self-control, (ii) a model including low self-control and demographic variables, (iii) a model including low self-control and online routine activities, and (iv) a full model, including low self-control, demographic variables and online routine activities.

In logistic regression analysis, unstandardized coefficients between different models can change even if omitted variables are not related to the independent variables. Therefore, contrary to common research practice, these coefficients cannot be compared. Following Mood's (2010) suggestion, I made logistic regression coefficients comparable across models by dividing unstandardized coefficients with the standard deviation of the latent variable (sdY*). This is the sum of the standard deviation of the predicted logit and the assumed deviation of the error term [the latter always being 1.81, or $\sqrt{(\pi^2/3)}$]. This way, coefficients express the standard deviation-unit change in Y* for a one-unit change in the independent variable.

Table 3 shows several interesting results. Model 1 displays the bivariate association between low self-control and online consumer fraud victimization. This result makes clear that risks are substantially higher for impulsive respondents. The odds ratio, comparing the people with the lowest and highest amount of self-control (a one-unit difference within this scale variable), is 10.08. Models 2 and 3 show that the effect of low self-control on fraud victimization declines by including either demographic or online routine activity variables. In both cases, the y-standardized coefficient drops 23 per cent, from 1.06 to 0.82. The decline in the low self-control effect in Model 3 suggests that part of the reason why impulsive people run higher victimization risk is because they perform more risky online activities. In this model, we observe that Internet purchasing and visiting online forums are risk enhancing. Indeed, the results from Table 2 already made clear that these activities were performed more often by impulsive people. Model 2 (Table 3) reveals that fraud victimization is inversely related to age and positively related to educational level. The latter finding may suggest that higher educated people are more skilled in retrieving interesting commercial offers. While this skill may result in higher profits most of the time, it also results in greater probability to occasionally run into a 'lemon' (Titus, Heinzelmann and Boyle, 1995). The other demographic characteristics, such as sex, household income, and degree of urbanism of the respondent's residential environment do not exert any significant effects. In addition, the decline in the effect of low self-control in Model 2 makes clear that it is also tied to demographic characteristics that are related to risk. Indeed, according to additional analyses (data not shown), low self-control is more prominent among young people and the lower educated.[5]

Finally, Model 4 in Table 3 shows the results of the full model. First of all, it reveals a significant and positive effect of low self-control on online consumer fraud victimization. This finding shows that the higher risk among people with low self-control is not only due to their higher participation in risky online activities, as the model controls for that aspect. Apart from that, people with low self-control probably react differently to online commercial offers, by more quickly deciding to buy a product, for instance if there are no adequate terms of guarantee. With the inclusion of both the routine online activities and the demographic characteristics in the full model, the y*-standardized coefficient of the effect of low self-control drops a little further, from 0.82 to 0.76. Furthermore, age, educational level, online shopping, and online forum participation—the variables exerting significant effects in Models 2 and 3—remain significant in Model 4, with little change in their coefficients. Additional analyses (data not shown) reveal that the effect of low self-control is somewhat stronger for the selection of people likely to be targeted due to being active in online purchasing ($N = 3{,}563$). The odds ratio for self control is 7.31 in this model (OR = 7.11 for the full sample). This is in line with the findings in Holtfreter, Reisig and Pratt (2008), who suggests that

**Table 3** Logistic regression of Internet consumer fraud victimization on individual characteristics ($N = 6{,}201$)

| Variables | 1 Low self-control (LSC) | | | 2 LSC+demographics | | | 3 LSC+routine online act. | | | 4 Full model | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $B_{stdY}$ | Wald | Exp(B) | $B_{stdY}$ | Wald | Exp(B) | $B_{stdY}$ | Wald | Exp(B) | $B_{stdY}$ | Wald | Exp(B) |
| Low self-control | 1.06 | 40.33** | 10.08 | 0.82 | 27.10** | 7.76 | 0.82 | 25.61** | 6.97 | 0.76 | 24.01** | 7.11 |
| Female | – | – | – | −0.11 | 2.82 | 0.76 | – | – | – | −0.07 | 1.23 | 0.83 |
| Age | – | – | – | −0.01 | 19.94** | 0.97 | – | – | – | −0.01 | 6.37* | 0.98 |
| Educational level | – | – | – | 0.01 | 8.62** | 1.19 | – | – | – | 0.02 | 9.81** | 1.21 |
| Household size | – | – | – | 0.07 | 0.12 | 1.03 | – | – | – | 0.07 | 0.30 | 1.04 |
| Household income | – | – | – | −0.01 | 0.25 | 0.98 | – | – | – | −0.01 | 0.25 | 0.98 |
| Partner present in household | – | – | – | 0.02 | 0.01 | 1.02 | – | – | – | 0.03 | 0.01 | 0.98 |
| Degree of urbanism | – | – | – | −0.01 | 0.67 | 1.06 | – | – | – | −0.01 | 1.62 | 1.09 |
| Internet shopping (hours/week) | – | – | – | – | – | – | 0.18 | 25.55** | 1.53 | 0.15 | 20.37** | 1.48 |
| Visiting online forums (hours/week) | – | – | – | – | – | – | 0.08 | 15.21** | 1.22 | 0.07 | 13.61** | 1.21 |
| Social network site: Hyves | – | – | – | – | – | – | 0.09 | 1.37 | 1.24 | 0.01 | 0.01 | 1.02 |
| Social network site: Facebook | – | – | – | – | – | – | 0.27 | 1.70 | 1.89 | 0.19 | 1.05 | 1.65 |
| Social network site: Other site | – | – | – | – | – | – | −0.25 | 2.01 | 0.55 | −0.24 | 2.26 | 0.54 |
| Webcam | – | – | – | – | – | – | 0.07 | 0.62 | 1.18 | 0.07 | 0.68 | 1.19 |
| −2 log likelihood | | 1,394.81 | | | 1,360.72 | | | 1,340.79 | | | 1,320.35 | |
| Nagelkerke $R^2$ | | 0.026 | | | 0.053 | | | 0.068 | | | 0.083 | |

*$P < 0.05$, **$P < 0.01$ (two-sided).

low self-control has stronger effects among people being targeted by offenders.

In order to show how the effects from the logistic models translate into easier interpretable victimization probabilities, Table 4 offers an overview of the predicted risks of Internet consumer fraud for various respondent profiles. For these profiles, characteristics significantly associated with fraud in Table 3 (Model 4)—age, educational level, online shopping, participation in online forums, impulsivity—are varied, which results in clearly different risk predictions. For instance, a profile that combines all risk enhancing characteristics—low self-control, active shopper, etc.—results in a predicted risk of 43 per cent. Conversely, the counterpart profile, combining all risk-decreasing characteristics results in a predicted risk of 0.6 per cent.[6] Table 4 also includes four different 'mixture' profiles, with predicted risks ranging from 3.8 per cent to 10.1 per cent.

## Conclusions

In a 1-year period, about 2.5 per cent of Dutch Internet users in the age group ≥16 years bought a product online and did not receive the ordered goods. With 90 per cent of all Dutch households having Internet access (Bureau of Statistics, 2009), the estimate is that the annual number of online consumer fraud victims in The Netherlands is approximately 300 thousand. This makes clear that Internet consumer fraud victimization is a serious problem. Apart from the financial loss for fraud victims, there is reason to suggest that negative e-commerce experiences lead to less social cohesion because they decrease generalized trust (Mutz, 2009). As of yet, little research has been conducted on such online consumer fraud victimization. This article tries to explain why some groups are more vulnerable to this kind of deception than others.

Self-control theory, originally formulated by Gottfredson and Hirschi (1990) as a theory of offending, was reformulated by Schreck (1999) to argue that low self-control also affected chances of crime *victimization*. The results of the current study are clearly in accordance with his predictions, showing that people with low self-control run higher fraud victimization risks. Routine activity theory (Cohen and Felson, 1979) was used to account for the association between low self-control and victimization, by suggesting that impulsive people are more vulnerable to crime because they engage more in risk enhancing Internet activities, such as online purchasing. Although there was some support for that explanation, an independent relation remained between low self-control and Internet consumer fraud

**Table 4** Predicted probabilities of Internet consumer fraud victimization for various respondent profiles

| Respondent profile | Predicted probability of victimization (per cent) |
|---|---|
| Age 20 years, academic education, active online shopper, active forum participant, low self-control | 43.1 |
| Age 20 years, academic education, active online shopper, non-participant in forums, high self-control | 9.9 |
| Age 20 years, low education, active online shopper, non-participant in forums, low self-control | 10.1 |
| Age 60 years, academic education, non-shopper, active forum participant, high self-control | 3.8 |
| Age 60 years, low education, active online shopper, non-participant in forums, low self-control | 4.8 |
| Age 60 years, low education, non-shopper, non-participant in forums, high self-control | 0.6 |

victimization after controlling for these activities. This suggests that impulsive people respond differently to deceptive online commercial offers, compared to less impulsive people (e.g. more aimed towards product purchase). Future experimental research may shed further light on this finding by presenting respondents the same online offers—varying in trustworthiness—and invite them to elaborate on which ones they would consider for the purchase of a product.

As expected from a routine activity perspective, Internet purchasers run more risk at fraud victimization. A more surprising finding is that active online forum participants are also more vulnerable to this, after controlling for a host of other risk factors. Possibly, a target's forum participation provides a certain group of offenders, visible cues on who is easily deceived or interested in taking risks. Again, future research could elaborate on this point by asking respondents more precise information on the type of information they share in online communities and Internet profiles. Research among American university students has shown, for instance, that it is not unusual for young people to share a large amount of personal information on the Internet (Irani *et al.*, 2009).

Internet auction sites as well as online consumers can realize situational crime prevention by adopting various strategies (Newman and Clarke, 2003). Online auctions for instance have established possibilities for customer feedback by rating options for satisfaction with specific sellers, and sometimes auction sites refuse sellers with negative feedback records. Other widely introduced examples are electronic payment methods that are safer than cash transactions (Paypal), as well as possibilities to handle transactions by a trusted third party provided by the site, which ensures that goods are deliverd first before payment (escrow service). Online customers can also play an important role by handling in ways to minimize fraud victimization risk, such as trying to realize face-to-face contact with the seller, no cash payments in remote transactions, use third party services—especially if the stakes are high—and gain information from community sites that record fraud tactics in specific cases. Future studies in this field should focus on these types of target preventive behaviour during the transaction, in order to assess if they are indeed effective in reducing victimization.

Still, it should be noted that, despite these possibilities for prevention, the present study suggests that low self-control plays an important role in shaping vulnerability to fraud. The precautions mentioned above are probably paid less attention to by people with low self-control, as this group anticipates less to possible negative outcomes in the distant future (Baumeister, 2002). Low self-control is generally viewed as stable throughout the life course, at least during adulthood (Gottfredson and Hirschi, 1990). Therefore, despite the possibilities for situational prevention for the general population, the stability of risk enhancing personality characteristics would put a limit to the prevention of fraud for some groups. In order to explore this prediction, future studies should study behavioural modification after fraud victimization, or the possible lack thereof among impulsive people. For this reason, low self-control may be associated with sustained risk over time for *repeat* victimization of online consumer fraud. Though longitudinal data collection is rare in victimization research, it is warranted in order to answer these kind of relevant questions.

## Notes

1. According to Felson and Clarke (1998), the general suitability of a crime target is determined by the acronym VIVA: *value*, *inertia*, *visibility*, and *accessibility*.
2. The reference population for the LISS panel is the Dutch speaking population permanently residing in The Netherlands. A random sample of 10,150 addresses was drawn from this population. After an announcement letter, households were contacted for a recruitment interview by CATI or by CAPI (if a telephone number was unknown). For 75 per cent of the households, a contact person answered questions for this recruitment interview. Of these households, 63 per cent registered as a member of the LISS panel, leading to a total number of 9,831 eligible household members. Respondents received a €10 incentive if they participated in the recruitment interview and an additional €10 if they registered as panel member (Scherpenzeel, 2009).
3. The sample showed a slight underrepresentation of males, the youngest (15–24 years) and oldest (≥65 years) respondents, as well as respondents from the most urban and rural regions. To optimize the estimate on the prevalence of online consumer fraud, data weighting for gender, age, and urbanism was applied to correct for discrepancies between the sample and the general population.
4. Fifteen per cent of victims were repeat victims within this 1-year period. To establish if risk factors operate differently when it comes to the *frequency* of victimization, I performed alternative regression analyses using a count measure as the dependent variable. Considering the skewed nature of this variable, a negative binomial model was used. Results were highly similar to those from the logistic models.
5. Also, these demographic characteristics are related to the online activities in Model 3. For instance, young people make more online purchases than older people. Thus, these results are in line with the prediction that self-control selects people into certain types of routine activities. Also, they support Hindelang, Gottfredson and Garofalo *et al.*'s (1978) lifestyle model, which argues that demographic characteristics predict the roles people play in everyday life, and which activities they perform.
6. For the most at-risk profile, impulsivity was set at the 95th percentile, active shopping at 3 h per week, active forum participation at 5 h per week, young age at 20 years and education at the academic level. For the least at-risk profile, impulsivity was set at non-impulsive; online shopping and participation in forums at 0 h per week, old age at 60 years and education at lower school.

## Acknowledgements

I thank two anonymous reviewers for their helpful comments on an earlier draft of this paper.

## References

Anderson, K. B. (2004). *Consumer Fraud in the United States: An FTC Survey*. Washington: Federal Trade Commission.

Anderson, K. B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy and Marketing*, **25**, 160–171.

Anderson, K. B. (2007). *Consumer Fraud in the United States: The Second FTC Survey*. Washington: Federal Trade Commission.

Baumeister, R. F. (2002). Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior. *Journal of Consumer Research*, **28**, 670–676.

Brown, J. R. and Goolsbee, A. (2002). Does the Internet make markets more competitive? Evidence from the life insurance industry. *Journal of Political Economy*, **110**, 481–507.

Bureau of Statistics (2008). *De Digitale Economie 2008 [The Digital Economy 2008]*. The Hague: Bureau of Statistics.

Bureau of Statistics (2009). *De Digitale Economie 2009 [The Digital Economy 2009]*. The Hague: Bureau of Statistics.

Caci, H. *et al.* (2003). Functional and dysfunctional impulsivity: Contribution to construct validity. *Acta Psychiatric Scandinavia*, **107**, 34–40.

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

Dickman, S. J. (1990). Functional and dysfunctional impulsivity: personality and cognitive correlates. *Journal of Personality and Social Psychology*, **58**, 95–102.

Felson, M. and Clarke, R. V. (1998). *Opportunity Makes the Thief: Practical Theory for Crime Prevention*. London: Home Office.

Forde, D. R. and Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly*, **14**, 265–294.

Forrester Research (2007). *The State of Retailing Online 2007*. Washington DC: The 10th Annual Shop.org Study.

Gottfredson, M. R. and Hirschi, T. (1990). *A General Theory of Crime*. Stanford: Stanford University Press.

Heaven, P. C. L. (1993). Personality predictors of self-reported delinquency. *Personality and Individual Differences*, **14**, 67–76.

Hindelang, M., Gottfredson, M. R. and Garofalo, J. (1978). *Victims of Personal Crime*. Cambridge, MA: Ballinger.

Holt, T. J. and Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, **30**, 1–25.

Holtfreter, K., Reisig, M. D. and Blomberg, T. G. (2006). Consumer fraud victimization in Florida: an empirical study. *St.Thomas Law Review*, **18**, 761–789.

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

Holtfreter, K., van Slyke, S. and Blomberg, T. G. (2005). Sociolegal change in consumer fraud: from victim-offender interactions to global networks. *Crime, Law and Social Change*, **44**, 251–275.

Holtfreter, K. *et al.* (2010). Low self-control and fraud: Offending, victimization, and their overlap. *Criminal Justice and Behavior*, **37**, 188–203.

Horrigan, J. B. (2008). *Online Shopping*. Washington: Pew Internet and American Life Project.

Internet Crime Complaint Center (2008). *Internet Crime Report 2008*. Washington, DC: The National White Collar Crime Center and the Federal Bureau of Investigation.

Irani, D. *et al.* (2009). Large online social footprints – An emerging threat. *Paper Presented at the 2009 International Conference on Computational Science and Engineering (CSE), Vancouver*, **3**, 271–276.

Junger, M., West, R. and Timman, R. (2001). Crime and risky behavior in traffic: an example of cross-national consistency. *Journal of Research in Crime and Delinquency*, **38**, 439–459.

Langenderfer, J. and Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: a new theory of visceral influences on persuasion. *Psychology and Marketing*, **18**, 763–783.

Meerkerk, G. J. *et al.* (2010). Is compulsive Internet use related to sensitivity to reward and punsihment, and impulsivity? *Computers in Human Behavior*, **26**, 729–735.

Mood, C. (2010). Logistic regression: why we cannot do what we think we can do, and what we can do about it. *European Sociological Review*, **26**, 67–82.

Mustaine, E. E. and Tewksbury, R. (1998). Predicting risks of larceny theft victimization: a routine activity analysis using refined lifestyle measures. *Criminology*, **36**, 829–857.

Mutz, D. C. (2009). Effects of Internet commerce on social trust. *Public Opinion Quarterly*, **73**, 439–461.

Newman, G. R. and Clarke, R. V. (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton: Willan.

Oudejans, M. and Vis, C. (2008). *Slachtoffers van (Poging tot) Oplichting [Victims of (Attempts at) Fraud]*. The Hague: WODC.

Piquero, A. R. *et al.* (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology*, **21**, 55–71.

Pratt, T. C., Holtfreter, K. and 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**, 267–294.

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

Scherpenzeel, A. (2009). *Start of the LISS panel. Sample and Recruitment of a Probability-based Internet Panel*. Tilburg: CentERdata.

Schreck, C. J. (1999). Criminal victimization and low self-control: an extension and test of a general theory of crime. *Justice Quarterly*, **16**, 633–654.

Schreck, C. J., Stewart, E. A. and Fisher, B. S. (2006). Self-control, victimization, and their influence on risky lifestyles: a longitudinal analysis using panel data. *Journal of Quantitative Criminology*, **22**, 319–340.

Stewart, E. A., Elifson, K. W. and Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly*, **21**, 159–181.

Titus, R., Heinzelmann, F. and Boyle, J. M. (1995). The anatomy of fraud: report of a nationwide survey. *National Institute of Justice Journal*, **229**, 28–36.

Trahan, A., Marquart, J. W. and Mullings, J. (2005). Fraud and the American dream: toward an

understanding of fraud victimization. *Deviant Behavior*, **26**, 601–620.

van Dijk, J., van Kesteren, J. and Smit, P. (2007). *Criminal Victimisation in International Perspective. Key Findings from the 2004-2005 ICVS and EU-ICS*. The Hague: WODC.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, **8**, 115–127.

Vigil-Colet, A. and Morales-Vives, F. (2005). How impulsivity is related to intelligence and academic achievement. *Spanish Journal of Psychology*, **8**, 199–204.

Weltevreden, J. (2007). *Winkelen in het Internettijdperk [Shopping in the Internet Age]*. Rotterdam: NAi Uitgevers.