Preventive Medicine Reports 17 (2020) 101058

Contents lists available at ScienceDirect

Preventive Medicine Reports

journal homepage: www.elsevier.com/locate/pmedr

Risk and protective factors of identity theft victimization in the United States

David Burnes[a,*], Marguerite DeLiema[b], Lynn Langton[c]

[a] University of Toronto, Factor-Inwentash Faculty of Social Work, 246 Bloor Street West, Toronto, Ontario, M5S1V4, Canada
[b] University of Minnesota, Twin Cities, School of Social Work, 105 Peters Hall, 1404 Gortner Ave., St. Paul, MN, 55108, USA
[c] RTI International, Division for Applied Justice Research, 701 13th Street NW, Washington DC, 20005, USA

ARTICLE INFO

Keywords:
Identity theft victimization
Risk factors
Protective factors
United States

ABSTRACT

Identity theft victimization is associated with serious physical and mental health morbidities. The problem is expanding as society becomes increasingly reliant on technology to store and transfer personally identifying information. Guided by lifestyle-routine activity theory, this study sought to identify risk and protective factors associated with identity theft victimization and determine whether individual-level behaviors, including frequency of online purchasing and data protection practices, are determinative of victimization. Data from sequential administrations of the U.S. National Crime Victimization Survey–Identity Theft Supplement (ITS) in 2012 and 2014 were combined (N = 128,419). Using multivariable logistic regression, risk and protective factors were examined for three subtypes: 1) unauthorized use of existing credit card/bank accounts, and unauthorized use of personal information to 2) open new accounts, or 3) engage in instrumental activities (e.g., applying for government benefits, receiving medical care, filing false tax returns). Existing credit card/bank accounts and new accounts identity theft victimization were associated with higher levels of online purchasing activity and prior identity theft victimization. All identity theft subtypes were associated with government/corporate data breaches and other crime victimization experiences. Routine individual-level preventive behaviors such as changing online passwords and shredding/destroying documents were protective. Identity theft subtypes showed divergent socio-demographic risk/protective profiles, with those of higher socioeconomic status more likely to be victims of existing credit card/bank account identity theft. Identity theft is a pervasive, growing problem with serious health and psychosocial consequences, yet individuals can engage in specific protective behaviors to mitigate victimization risk.

1. Introduction

Identity theft – defined as the intentional, unauthorized use of a person's identifying information for unlawful purposes (Federal Trade Commission, 1998; Koops and Leenes, 2006) – is a growing public health problem. While identity theft is not a new crime, the magnitude of the problem has increased with society's growing reliance on the electronic transfer and storage of personal information across all forms of commerce and services. Approximately 10% of U.S. adults experienced identity theft in 2016, up from 7% in 2012 (Harrell, 2019), and consumer agencies have seen recorded complaints about identity theft increase almost five-fold since 2001 (Federal Trade Commission, 2017). Even routine, mandatory interactions with government (e.g., filing taxes) and healthcare systems (e.g., health records) involve the online transfer and storage of highly identifiable information, such as social security and medical ID numbers, expanding opportunities for identity thieves to illegally obtain personal information (Myers et al., 2008).

In addition to the rising incidence of identity theft, there is growing recognition of the negative emotional and physical health consequences of financial crimes. One in 10 identity theft victims, roughly 2.6 million people, reported experiencing severe emotional distress following victimization (Harrell, 2019). A quarter of identity theft victims experienced sleep problems, anxiety, and irritation six months after the crime (Sharp et al., 2004), with older adults and minorities experiencing more severe emotional consequences including depression, anger, worry, and sense of vulnerability (Golladay and Holtfreter, 2017). While not specific to identity theft, Ganzini and colleagues (1990) found significantly higher rates of depression and anxiety among financial crime victims compared to demographically-matched controls. Financial crimes have also been associated with increased rates of hospitalization (Dong and

* Corresponding author.
E-mail addresses: david.burnes@utoronto.ca (D. Burnes), mdeliema@umn.edu (M. DeLiema), laustell@rti.org (L. Langton).

https://doi.org/10.1016/j.pmedr.2020.101058
Received 30 July 2019; Received in revised form 12 January 2020; Accepted 21 January 2020
Available online 23 January 2020

Simon, 2013) and all-cause mortality (Burnett et al., 2016). Identity theft also diminishes public confidence in government and corporate entities, prompting increasingly restrictive access to government databases designed to promote public health research (Wartenberg and Thompson, 2010).

The large number of high-profile data breaches in the 21st century (e.g., Equifax, Yahoo, Anthem, U.S. Office of Personnel Management) introduce the question of whether individual-level characteristics and behaviors affect the risk of identity theft victimization, or whether victimization risk is entirely contingent on corporate and government-level data security practices. Combining 2012 and 2014 data from the Bureau of Justice Statistics' (BJS) nationally representative *National Crime Victimization Survey – Identity Theft Supplement* (NCVS-ITS), the current study provides a comprehensive examination of identity theft victimization risk and protective factors across three major identity theft subtypes: 1) Unauthorized use of existing credit card(s) and/or bank account(s) and; Unauthorized use of personal information to 2) open new account(s); or 3) engage in instrumental activities. Although the BJS provides basic descriptive and bivariate statistics from the NCVS-ITS with a focus on socio-demographic variables, a multivariable analysis is necessary to identify whether individual-level online routines and lifestyle behaviors affect the probability of victimization above and beyond risk factors that are largely outside of an individual's control, such as corporate/government-level data breaches. Only through this more comprehensive analysis that isolates the impact of individual behaviors after controlling for other factors can we begin to understand where to effectively allocate security resources to help reduce the frequency and consequences of identity theft. In contrast to BJS reports that combine both "attempted" and "actual" cases of identity theft in analysis, the current study focuses on identity theft victimization and, therefore, includes only cases of actual identity theft (excluding attempted cases).

2. Theoretical framework

The current paper draws on lifestyle-routine activity theory (L-RAT; Cohen and Felson, 1979; Hindelang et al., 1978) which proposes that individual lifestyles and routine activities influence the risk of crime victimization to the extent that they bring a potential target into contact with offenders or affect the availability of protective measures to prevent the crime (Cohen et al., 1981; Miethe & Meier, 1990; Hindelang et al., 1978). L-RAT originally described crimes involving direct victim-perpetrator contact, such as assault and robbery, yet the theory has been modified for application to internet-based crimes in which the victim and perpetrator do not physically or necessarily instantaneously converge, including financial fraud (Pratt et al., 2010) and identity theft (Reyns, 2013; Reyns and Henson, 2016).

According to L-RAT, individuals with greater visibility to offenders in unguarded/un-protected settings are more likely to be victimized (Cohen et al., 1981). In the context of cyber crimes, online activity could expose a person's identifying information to offenders if the device is infected with malware, hacked, or personal data is entered into an unsecure website. Identity theft research has generally supported the hypothesis that engagement in routine online commercial activities, such as banking, shopping, emailing/instant messaging, selling goods, downloading media, or higher overall levels of internet usage, is associated with victimization (Holtfreter et al., 2014; Reyns, 2013; Reyns and Henson, 2016; Williams, 2016). Yet beyond individual online activities, data breaches targeting retailers, healthcare insurers/providers, and government entities that store and transfer personal information may also increase risk of identity theft.

Previous studies examining L-RAT and criminal behavior have found that routine activities account for a substantial portion of the association between crime and socio-demographic characteristics (Osgood et al., 1996). It is unknown whether identity theft victimization is correlated with demographic and socioeconomic characteristics—age, income, education, race, residential setting—given that personal information is often obtained through online channels with no direct victim-perpetrator contact. Yet these characteristics influence socio-cultural lifestyles and patterns of consumption that affect how often individuals use their identifying information and for what purposes. Previous researchers have found a positive relationship between income, educational attainment, and identity theft victimization (Anderson 2006; Reyns, 2013; Reyns & Henson, 2016; Williams, 2016).

Prior studies have inconsistently found that both females (Anderson, 2006) and males (Holtfreter et al., 2014; Reyns, 2013) are at greater risk of identity theft victimization. Similarly, different studies have shown that younger adults (Williams, 2016), middle-aged adults (Harrell, 2015), and older adults (Reyns, 2013) are at increased risk of victimization. Rather than considering age as a continuous variable or according to arbitrary cut-offs, the current study examined age according to generational cohorts, which may be more indicative of age-cohort-related lifestyles and routine activity trends. The study also examined age and gender risk profiles separately for each identity theft subtype, as differences in how information is obtained and misused could explain previous mixed findings.

According to L-RAT, people with greater measures of protection or security, including social, physical, or safety measures are at lower risk of victimization (Cohen et al., 1981; McNeeley, 2015; Wilcox et al, 2007). In the context of identity theft, behaviors such as installing antivirus software, shredding documents, and routinely changing passwords theoretically reduce opportunities for identity thieves to access personal information. This has received mixed results in the identity theft literature. Reyns and Henson (2016) found that protective computer/internet-based behaviors, such as use of antivirus software, deleting emails from unknown senders, and regularly changing passwords, were not related to identity theft victimization. Williams (2016) found that some security measures (using only one computer, filtering spam email, installing antivirus software and secure browsing) were associated with lower identity theft victimization, while other measures (changing security settings and passwords) were associated with greater victimization. However, existing identity theft research is limited by study designs that have been unable to determine whether reported protective behaviors were enacted as a general precautionary measure (prior to) or in response to (following) identity theft victimization. The current study only considered protective behaviors reported as general preventive measures and excludes protective behaviors enacted in reaction to a victimization experience.

3. Methods

3.1. Data

This study combined cross-sectional data (n = 128,419) from a rotating panel design of consecutive, directly comparable 2012 (n = 64,132) and 2014 (n = 64,287) administrations of the NCVS-ITS (U.S. Department of Justice, 2012, 2014). The broader NCVS study used a two-stage, stratified cluster sample design, representing all U.S. residents age 12 years or older living in housing units or group quarters. The ITS surveys were administered to eligible respondents age 16 or older at the end of their NCVS interviews using computer-assisted personal or telephone interviewing. While the ITS survey collected only data about respondent experiences with identity theft, respondents' demographic data and their experiences with other types of crime victimization were collected through the broader NCVS survey. The overall NCVS-ITS unit response rates for NCVS households, NCVS persons, and ITS persons in 2012 and 2014 were 68.2% and 66.1%, respectively. Selection bias analysis found little or no bias to ITS estimates due to non-response (Inter-University Consortium for Political and Social Research [ICPSR], 2012, 2014). Data were weighted to be nationally representative but adjusted back to reflect the original sample

size and avoid inflated p-values. Further details on NCVS-ITS methods can be found at www.bjs.gov (Bureau of Justice Statistics, 2014).

3.2. Dependent variables

Consistent with empirically derived recommendations to maximize sensitivity and reduce respondent under-reporting in financial exploitation prevalence research (Burnes et al., 2017), the NCVS-ITS measured identity theft victimization using a series of contextually oriented questions describing specific sub-categories, rather than a single, general self-report assessment question. Dependent identity theft variables include the unauthorized use of: 1) existing credit card and/or bank accounts; 2) personal information to open new accounts (e.g., financial, investment, utilities); and 3) personal information for instrumental purposes (e.g. filing false tax returns, obtaining medical services, applying for a job or government benefits). Because the mechanisms of identity exposure and the purposes of identity misuse differ across these three categories, risk and protective factors were assessed separately in the analysis. Victimization status was limited to respondents reporting identity theft within the previous year (1 = yes, 0 = No).

3.3. Independent variables

3.3.1. Risk factors

Potential risk factors for identity theft included: 1) frequency of online purchasing behavior in the past year (none, up to once per month, up to once per week, up to once per day, more than once per day); 2) prior year breach of personal information stored by a company or government (no = 0, yes [but social security number not exposed] = 1, yes [social security number exposed] = 2); 3) number of other forms of victimization experienced in the past year, such as theft and assault (continuous); and 4) whether the respondent experienced prior identity theft victimization during lifetime (yes = 1, no = 0).

3.3.2. Protective factors

Respondents were asked a series of seven questions (no = 0/ yes = 1) designed to capture identity theft-related preventive/protective practices within the previous 12 months. The questions asked about the following behaviors: checked credit report; changed passwords on financial accounts; purchased credit monitoring services or identity theft insurance; shredded or destroyed documents containing personally identifying information; checked bank or credit card statements for unfamiliar charges; used computer security software; or purchased identity theft protection services. An affirmative response to each question triggered a follow-up question asking whether the behavior was enacted in response to a misuse of personal information. To address issues of temporal ordering as it relates to routine protective behaviors, respondents who indicated that a behavior was enacted in response to a victimization event in the past 12 months were coded as a “no” for the preventive behavior. To understand whether the seven binary protective practice items loaded onto one or more dimensional factors, a multiple correspondence analysis (MCA) was conducted, which analyzed the underlying structure of the binary/categorical data (Greenacre & Blasius, 2006). As illustrated in the discrimination measures plot (Appendix A), two factors emerged based on whether the protective item was purchased or reflected a routine protective behavior. The *purchased* factor contained two items—credit monitoring services/identity theft insurance and identity theft protection services. The *routine protective behavior* factor had five items—checked credit report, changed passwords, shredded/destroyed documents, checked bank/credit card statements, used computer security software. These *purchase* and *routine protective behavior* variables (continuous) were entered separately into the models.

3.3.3. Controls

Age was operationalized according to generational cohorts to reflect age-related lifestyles that could impact exposure to identity theft: millennials (born 1981–1998), Generation X (born 1965–1980), baby boomers (born 1946–1964), and Silent/Greatest (born before 1945) (Pew Research Center, 2016). Additional socio-demographic characteristics included gender (male/female), marital status (married/ partnered vs. not married/partnered), education (high school or less, some college, college degree, advanced degree), annual household income ($0–24,999, $25,000–49,999, $50,000–74,999, $75,000 or more), and race/ethnicity (non-Hispanic white, non-Hispanic black, Hispanic, non-Hispanic Asian American/Pacific Islander/American Indian/Alaska Native [AAPI/AIAN], other). Other control variables included residential setting (urban, rural) and survey administration mode (in-person, telephone).

3.4. Analytic plan

Risk and protective variables and controls were regressed on each subtype of identity theft using multivariable logistic regression. Model fit was tested using the Omnibus Test of Model Coefficients and the Hosmer-Lemeshow Test. Tolerance and variance inflation factor statistics were used to test for multicollinearity in regression models. The existing credit card/ bank account analysis was limited to respondents who reported having a credit card or bank account. Missing data were managed with a fully conditional specification multiple imputation method using five pooled data sets. Analyses were performed using IBM SPSS version 25. Due to the large sample size, a p-value of less than 0.001 was considered statistically significant.

4. Results

Table 1 provides a description of the weighted sample of victims across identity theft subtypes. Across identity theft subtypes, victims were proportionally more female, Caucasian, belonged to the Baby Boomer generation, and lived in urban settings. Whereas victims of existing credit card/bank account identity theft tended to belong to higher income households, victims of new accounts and instrumental purposes identity theft tended to belong to lower-income households.

Table 2 presents the prevalence of identity theft victimization overall and by subtype. The prevalence of overall identity theft victimization (any type) was 6.2% in the combined 2012/2014 sample (95%CI = 6.0%–6.3%). The most common form of victimization was existing credit card or bank account identity theft, with a prevalence of 5.6% (95%CI = 5.5%–5.8%).

4.1. Risk factors

Table 3 presents results from the multivariable analysis of risk and protective factors of identity theft victimization for each subtype. Higher levels of online purchasing behavior were significantly associated with increasing odds of existing credit card/bank account and new accounts identity theft victimization; those engaging in daily online shopping were more than five times as likely to be victims of existing credit card/bank account identity theft as those not engaging in online purchasing (OR = 5.74, 95%CI = 4.31–7.64). Persons reporting breached personal information from a company or government were significantly more likely to experience identity theft, particularly if social security information was exposed (instrumental purposes: OR = 8.05, 95%CI = 5.66–11.46; new accounts: OR = 3.83, 95%CI = 2.67–5.51; existing credit/bank account: OR = 1.46, 95%CI = 1.26–1.68). Those reporting other NCVS victimizations were between 29% (existing credit/bank account: OR = 1.29, 95%CI = 1.23–1.35) and 46% (new accounts: OR = 1.46, 95%CI = 1.32–1.62) more likely to be victims of identity theft with each successive crime. Individuals with a history of identity theft

Table 1
Descriptive characteristics of weighted (sample-size-adjusted) victim samples across identity theft victimization subtypes.

	Existing Credit Card or Bank Account Victims (n = 7241)	New Accounts Victims (n = 492)	Instrumental Purposes Victims (n = 350)
Independent Variables	n (%), Mean (SD)	n (%), Mean (SD)	n (%), Mean (SD)
Risk Factors			
Online purchasing behavior frequency			
None (0 times/year)	1393 (19.2%)	191 (38.8)	156 (44.7)
Up to once per month (1–12 times/year)	2761 (38.1%)	169 (34.5)	110 (31.6)
Up to once per week (13–52 times/year)	2070 (28.6)	88 (17.9)	45 (12.8)
Up to once per day (58–365 times/year)	777 (10.7	31 (6.3)	25 (7.2)
More than once per day (More than 365 times/year)	62 (0.8)	5 (1.0)	4 (1.1)
Number of other victimizations (cont. 0–10)	0.1 (0.4)	0.2 (0.6)	0.2 (0.6)
Breached personal information	6027	400	271
No	(83.2%)924	(81.3)	(77.4)
Yes (SSN not exposed)	(12.8)	53 (10.8)	33 (9.4)
Yes (SSN exposed)	229 (3.2)	35 (7.1)	42 (12.1)
Identity theft victimization prior to past year			
No	5987 (82.7)	406 (82.6)	291 (83.1%)
Yes	1209 (16.7)	81 (16.5)	55 (15.8)
Protective Factors			
Purchase protective services (0–5)	0.1 (0.3)	0.1 (0.4)	0.1 (0.4)
Routine protective behaviors (0–5)	2.3 (1.4)	1.6 (1.5)	1.7 (1.5)
Controls			
Age generations	1706	1902	141
Millennials	(23.6)	(24.0%)2449	(28.8)
Generation X	2244 (31.0)	(30.9)	140 (28.4)
Baby boomers	2612 (36.1)	2832 (35.8)	165 (33.6)
Silent or Greatest	678 (9.4)	738 (9.3)	45 (9.2)
Gender	3461	3770	235
Male	(47.8)	(47.6%)	(47.7)
Female	3780 (52.2)	4152 (52.4)	257 (52.3)
Marital status	4384	4671	225
Married	(60.5)	(59.1%)	(45.7)
Non-married	2837 (39.2)	3229 (40.9)	267 (54.3)
Educational attainment			
High school or less	1605 (22.2)	1867 (23.7%)	135 (38.5)
Some college or associate degree	2152 (29.7)	2388 (30.3)	124 (35.5)
Bachelor's degree	2155 (29.8)	2270 (28.8)	63 (18.0)
Graduate/professional degree	1295 (17.9)	1360 (17.2)	26 (7.4)
Race/ethnicity	5591	289	206
White[a]	(77.2)	(58.7)	(58.9)
Hispanic	610 (8.4)	75 (15.2)	45 (12.8)
Black[a]	536 (7.4)	84 (17.1)	79 (22.5)
AAPI/AIAN*	393 (5.4)	20 (4.0)	13 (3.8)
Other*	112 (1.5)	24 (4.9)	7 (2.1)
Household income	668	114	86
$0–24,999	(9.2)	(23.2)	(24.5)
$25,000–49,999	1199 (16.6)	105 (21.3)	81 (23.0)
$50,000–74,999	1090 (15.1)	63 (12.7)	41 (11.7)
$75,000+	2934 (40.5)	117 (23.9)	66 (18.8)
Number of household members ≤ 12 years (cont. 0–9)	0.4 (0.8)	0.54 (0.95)	0.55 (1.01)
Residential setting			
Urban	6096 (84.2)	426 (86.6)	309 (88.4)
Rural	1145 (15.8)	66 (13.4)	41 (11.6)
Interview type	3170	254	197
In-person	(43.8)	(51.8)	(56.4)
Telephone	4071 (56.2)	237 (48.2)	153 (43.6)

[a] Excludes persons of Hispanic or Latino origin. AAPI/AIAN = Asian American/Pacific Islander/American Indian/Alaskan Native

Table 2
Identity theft victimization frequencies.

Identity Theft Victimization Subtype	Combined 2012/2014 (n = 128,419)
	n (%)
Any subtype	7921 (6.2)
Existing credit or bank account	7241 (5.6)
New accounts	492 (0.4)
Instrumental purposes	350 (0.3)

victimization were 28% more likely to be victimized by existing credit/bank account identity theft in the past year than those with no prior history (OR = 1.28, 95%CI = 1.19–1.37).

4.2. Protective factors

Individuals engaging in a higher number of proactive, routine protective behaviors, such as shredding documents and updating passwords, were between 25% (existing credit/bank account: OR = 0.76, 95%CI = 0.75–0.78) and 35% (new accounts: OR = 0.66, 95%CI = 0.61–0.71) less likely to experience identity theft victimization with each additional protective behavior. Purchasing credit monitoring services and identity theft insurance, however, was associated with significantly higher odds of new accounts (OR = 1.62,

Table 3
Multivariable logistic regression models predicting identity theft victimization.

Independent Variables	Existing Credit or Bank Account (n = 116,042)[a]	New Accounts (n = 128,419)	Instrumental (n = 128,419)
	OR (95% CI)	OR (95% CI)	OR (95% CI)
Risk Factors			
Online purchasing behavior frequency (ref. None)			
Up to once per month (1–12 times/year)	2.45 (2.28–2.63)***	1.71 (1.35–2.17)***	1.35 (1.02–1.78)
Up to once per week (13–52 times/year)	3.54 (3.27–3.83)***	1.78 (1.33–2.38)***	1.12 (0.77–1.64)
Up to once per day (58–365 times/year)	4.44 (4.02–4.90)***	1.89 (1.25–2.85)	2.01 (1.28–3.16)
More than once per day (More than 365 times/year)	5.74 (4.31–7.64)***	4.52 (1.79–11.46)	4.03 (1.39–11.70)
Number of other victimizations (cont.)	1.29 (1.23–1.35)***	1.46 (1.32–1.62)***	1.41 (1.24–1.60)***
Breached personal information (ref. No)			
Yes (SSN not exposed)	1.44 (1.33–1.56)***	1.96 (1.44–2.66)***	2.16 (1.47–3.19)***
Yes (SSN exposed)	1.46 (1.26–1.68)***	3.83 (2.67–5.51)***	8.05 (5.66–11.46)***
Identity theft victimization prior to past year (ref. No)	1.28	1.43	1.43
Yes	(1.19–1.37)***	(1.11–1.85)	(1.05–1.95)
Protective Factors			
Purchase protective services (cont.)	1.02 (0.95–1.09)	1.62 (1.28–2.06)***	1.37 (0.99–1.87)
Routine protective behaviors (cont.)	0.76 (0.75–0.78)***	0.66 (0.61–0.71)***	0.71 (0.65–0.78)***
Controls			
Age generations (ref. millennials)			
Generation X	1.21 (1.12–1.29)***	1.28 (1.00–1.65)	1.68 (1.26–2.24)***
Baby boomers	1.38 (1.29–1.48)***	1.70 (1.32–2.20)***	1.79 (1.32–2.42)***
Silent or Greatest	1.10 (0.99–1.21)	1.23 (0.86–1.78)	1.12 (0.72–1.75)
Gender (ref. Male)	0.99	0.95	1.14
Female	(0.94–1.04)	(0.79–1.13)	(0.92–1.42)
Marital Status (ref. Married/partnered)	0.95	1.23	1.63
Not married/partnered	(0.90–1.01)	(1.00–1.51)	(1.28–2.09)***
Educational attainment (ref. High school or less)			
Some college or associate degree	1.42 (1.33–1.52)***	1.70 (1.35–2.14)***	1.43 (1.11–1.86)
Bachelor's degree	1.67 (1.56–1.80)***	1.66 (1.25–2.20)***	1.18 (0.84–1.66)
Graduate/professional degree	1.90 (1.74–2.07)***	1.85 (1.31–2.61)	0.95 (0.59–1.50)
Race/ethnicity (ref. non-Hispanic white)			
Hispanic	0.85 (0.78–0.93)***	1.32 (1.00–1.73)	0.93 (0.66–1.32)
Black[b]	0.78 (0.71–0.86)***	1.43 (1.11–1.86)	1.58 (1.20–2.09)
AAPI/AIAN[b]	0.78 (0.70–0.87)***	0.73 (0.46–1.16)	0.69 (0.39–1.22)
Other[b]	1.09 (0.89–1.32)	3.32 (2.17–5.09)***	1.18 (056–2.50)
Household income (ref. $0 to 24,999)			
$25,000 to 49,999	1.05 (0.95–1.15)	0.77 (0.60–1.00)	0.90 (0.67–1.21)
$50,000 to 74,999	1.20 (1.08–1.33)	0.73 (0.54–0.99)	0.80 (0.56–1.13)
$75,000 +	1.38 (1.25–1.52)***	0.71 (0.52–0.97)	0.74 (0.52–1.05)
Number of household members ≤ 12 years (cont.)	1.01 (0.98–1.05)	1.20 (1.08–1.33)	1.21 (1.07–1.36)
Residential setting (ref. urban)	0.90	0.80	0.65
Rural	(0.84–0.96)	(0.61–1.05)	(0.46–0.91)
Interview type (ref. In-person)	0.91	0.85	0.74
Telephone	(0.87–0.96)***	(0.71–1.02)	(0.60–0.92)

Note: All multivariable logistic regression models, except the New Accounts model, satisfied the Omnibus Test of Model Coefficients ($p < 0.01$). All multivariable logistic regression models satisfied the Hosmer-Lemeshow Test ($p > 0.05$). Across models, independent variables had tolerance of 0.70 or above and variance inflation factor of 1.43 or below, indicating no concern of multicollinearity.
CI = Confidence interval; OR: Odds ratio; SSN: Social Security Number; AAPI/AIAN = Asian American/Pacific Islander/American Indian/Alaskan Native. ***$p < 0.001$, (two-tailed tests).
[a] Analysis of the existing credit or bank account subtype only includes NCVS-ITS respondents who reported having a credit card or bank account, respectively.
[b] Excludes persons of Hispanic or Latino origin.

95%CI = 1.28–2.06) identity theft.

4.3. Socio-Demographic controls

Across all identity theft subtypes, baby boomers were most likely to be victims (existing credit/bank account: OR = 1.38, 95%CI = 1.29–1.48; new accounts: OR = 1.70, 95%CI = 1.32–2.20; instrumental: OR = 1.79, 95%CI = 1.32–2.42). Unmarried/un-partnered persons were 63% (OR = 1.63, 95%CI = 1.28–2.09) more likely to experience instrumental forms of identity theft. Higher levels of education were associated with increasingly higher odds of both existing credit card/bank account and new accounts forms of identity theft. Compared to non-Hispanic whites, existing credit/bank account victimization was less likely among Hispanic (OR = 0.85, 95%CI = 0.78–0.93), Black (OR = 0.78, 95%CI = 0.71–0.86), and AAPI/AIAN (OR = 0.78, 95%CI = 0.70–0.87) persons. Persons living in households in the highest income bracket were most likely to experience existing credit/bank account identity theft (OR = 1.38, 95%CI = 1.25–1.52) compared to those in the lowest income households. As a methodological finding, respondents who participated in a telephone rather than in-person interview were significantly less likely to report identity theft victimization.

5. Discussion

Approximately 1 out of every 15 adults aged sixteen years or older in the U.S. – over 16 million people – experience some form of identity theft each year. In addition to direct losses, consequences may include damaged credit, legal fees, loss of trust, and health outcomes such as stress, anxiety, and depression (Harrell, 2015; Golladay & Holtfreter, 2017). Among victims who experienced the misuse of personal information for instrumental purposes, approximately 56% suffered moderate to severe distress, a similar percentage as seen among victims of violence (Harrell, 2015).

As large-scale data breaches have become an unfortunate part of our growing tech-based marketplace, this analysis examined whether online purchasing behavior and personal data security practices affect the risk of identity theft victimization, or whether becoming a victim is largely contingent on corporate and government-level data breaches. Findings provide support for the L-RAT model of victimization which suggests that individual lifestyle routines and degree of protective measures/guardianship influence the likelihood of victimization.

Respondents who stated that their information was part of a large data breach were significantly more likely to report all forms of identity theft, particularly when their social security numbers were exposed. Victims of identity theft for instrumental purposes were eight times as likely to say their social security numbers were exposed in a data breach compared to non-victims, likely because that form of identity theft requires social security numbers to access government benefits and other services. Although it is not possible to assess whether data breaches directly caused identity theft incidents, data breaches were significantly correlated with the misuse of identity information.

L-RAT proposes that routine lifestyle behaviors contribute to crime victimization risk. In the present study, individual risk and protective behaviors were consistent and strong (magnitude) predictors. Similar to findings using a Canadian sample (Reyns & Henson, 2016), increasing levels of online purchasing activity were associated with incrementally higher odds of financial account and new account identity theft. Participating in commercial activities online reflects a major societal innovation and lifestyle shift that has allowed consumers to purchase products conveniently and globally, but entering personal data online entrusts vendors to safely store and manage this data. For example, Holtfreter et al. (2015) found that individuals who placed an order with a company they had never done business with before were significantly more likely to be victims of identity theft. While the NCVS ITS does not ask respondents what online retailers they have made purchases from, it is likely that as the frequency of online shopping increases, the odds of using an unsecured payment portal or having information exposed in a retail data breach increases. Further innovations in online security and payment systems are required to protect users' information, and future research should explore precisely how online purchasing activities expose personal information.

In support of the guardianship principle of L-RAT, proactive individual behaviors, like shredding personal documents and routinely changing account passwords, significantly reduced the likelihood of identity theft. Unfortunately, the Pew Research Center (Olmstead & Smith, 2017) found that half of U.S. respondents were not educated about everyday security practices. Given that routine safety behaviors reduce risk of identity theft, consumer protection efforts need to focus on educating consumers on the basics of online security. Purchasing external credit monitoring and identity theft protection services did not reduce risk and was related to greater likelihood of new accounts identity theft victimization. Perhaps respondents who purchased these services had some knowledge that their identity may be misused. Another explanation is that some criminal entities have reached a level of sophistication to evolve techniques ahead of current industry protection standards (Moore et al., 2009).

This study found that exposure to other types of crime, as well as prior experiences with identity theft, were associated with a greater risk of identity theft victimization. Personal information may be stolen during the course of other crimes directly (e.g., theft of wallets, bank statements) or indirectly through theft of devices that contain personal information. This result is consistent with financial fraud research—prior fraud victimization increases the odds of re-victimization (Titus et al., 1995). An underground system exists for identity theft where specified pieces of stolen identifying information are bundled and sold to other criminals, thereby increasing the odds that it is used for various identity crimes over time (Moore et al., 2009). Services for identity theft victims should include help contacting the major credit bureaus to place a temporary freeze or fraud alert on credit reports to prevent criminals from opening new accounts with victims' stolen credentials.

The socioeconomic and demographic risk patterns found in this study were roughly consistent with the predictions of L-RAT. In general, members of Generation X and the baby boomers, now between the ages of 39 and 73, were at the highest risk of most types of identity theft. This likely reflects the socioeconomic capacity and consumption patterns among Generation X and baby boomers relative to millennials. Together, these older generations constitute the bulk of the U.S. workforce and, therefore, have the economic means to engage in consumer activities where identities may be exposed. Longitudinal data is needed to determine whether the association between middle to late adulthood and increased risk of identity theft is indeed due to lifestyles or whether age has an independent effect.

Compared to Hispanic, Black, and Asian respondents, White respondents and those with higher educational attainment experienced significantly higher risk of existing credit card/bank account identity theft. Individuals with higher socioeconomic status have more purchasing power (Charron-Chénier et al., 2017), have more access to credit (Haushofer & Fehr, 2014), own more internet-enabled devices that store and transfer personal information, and are more likely to use credit cards (Greene & Stavins, 2016). In support of L-RAT, this suggests that the association between existing credit card/bank account identity theft and demographic/socioeconomic profiles is related to lifestyle factors where there is greater reliance on these financial instruments, and thus more opportunities for criminals to intercept account information.

5.1. Limitations

While the NCVS Identity Theft Supplement is one of the most comprehensive sources of data on identity theft, the survey likely underestimates the true extent of the problem. First, the NCVS excluded adult sub-populations who may be particularly vulnerable, such as those living with cognitive impairment and/or in institutional settings. Second, the literature on financial fraud victimization finds that people tend to under-report victimization in survey research (Beals et al., 2015), and this self-report error likely extends to the issue of identity theft. Finally, the nonresponse group is likely disproportionately represented by victims who are reluctant to provide personal information in response to a survey. Another limitation of the study was that data on other potentially important behavioral variables, such as the extent of online downloading, online financial account management, types of websites visited, and presence of malware, hacking or phishing events, were unavailable. To better understand risk of identity theft victimization within the L-RAT paradigm, measures are needed to account for system-level security practices among corporate and government entities, but this is beyond the scope of the NCVS.

5.2. Health implications

Identity theft victimization affects tens of millions of Americans each year. Financial exploitation, in general, is associated with major health-related consequences such as increased rates of hospitalization and all-cause mortality. Victims of identity theft experience severe mental/emotional distress, particularly among minority and older adult populations (Harrell, 2019; Golladay & Holtfreter, 2017). Given the increasing scope of this problem, the development of effective primary prevention strategies is critically needed and should focus on promoting relatively unintrusive and feasible everyday practices such as routinely changing financial account passwords, shredding documents, and checking credit reports and financial statements. The prevalence of this problem indicates that healthcare professionals will encounter patients who are victimized by identity theft on a regular basis. Healthcare settings represent an important place to both recognize vulnerable adults and provide victims with preventive education to mitigate the

risk of identity exposure.

6. Conclusion

This study comprehensively examined the risk of different forms of identity theft victimization in the U.S. Although other research indicates that Americans have inadequate knowledge of cybersecurity practices (Olmstead & Smith, 2017), findings from the current study demonstrated the importance of this knowledge in keeping personal information safe. Yet individual actions alone are not enough. As investment in cybersecurity grows, criminals respond with increasingly sophisticated and evolving techniques such as hacking, malware, and skimming to overcome these controls (Pontell, 2009). Reducing the incidence of identity theft requires greater public/private investment in robust, dynamic data security systems and encryption tools, and more collaboration between criminal justice and law enforcement agencies to investigate and prosecute identity theft crimes.

CRediT authorship contribution statement

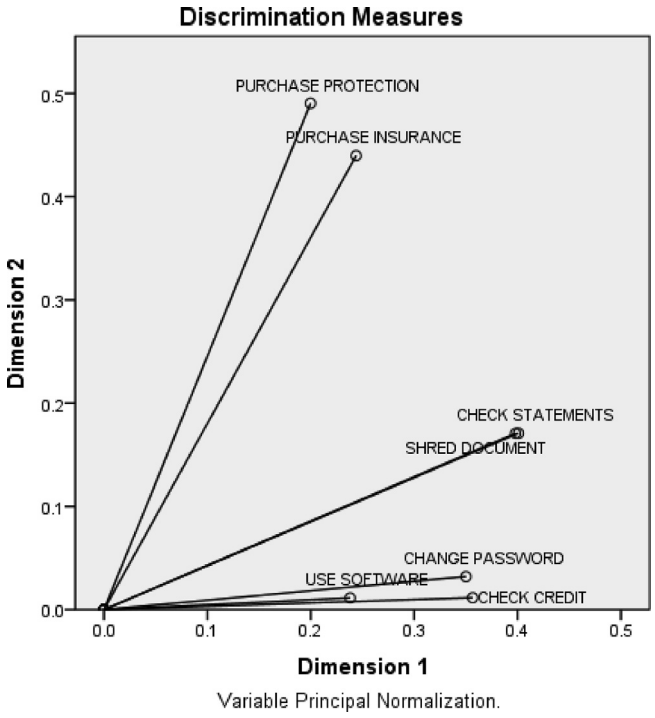
David Burnes: Conceptualization, Formal analysis, Data curation, Writing - original draft, Writing - review & editing. **Marguerite DeLiema:** Conceptualization, Writing - original draft, Writing - review & editing. **Lynn Langton:** Conceptualization, Methodology, Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A

Multiple Correspondence Analysis Discrimination Measures Plot.



Appendix B. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.pmedr.2020.101058.

References

Anderson, K., 2006. Who are the victims of identity theft? The effect of demographics. J. Public Policy Mark. 25 (2), 160–171.

Beals, M.E., Carr, D.C., Mottola, G.R., Deevy, M.J., Carstensen, L.L., 2015. How does survey context impact self-reported fraud victimization? Gerontologist 57 (2), 329–340. https://doi.org/10.1093/geront/gnv082.

Bureau of Justice Statistics, 2014. National Crime Victimization Survey: Technical documentation. Washington, DC: Bureau of Justice Statistics. https://www.bjs.gov/content/pub/pdf/ncvstd13.pdf (last accessed 1.5.20).

Burnes, D., Henderson Jr, C.R., Sheppard, C., Zhao, R., Pillemer, K., Lachs, M.S., 2017. Prevalence of financial fraud and scams among older adults in the United States: a systematic review and meta-analysis. Am. J. Public Health 107 (8), e13–e21. https://doi.org/10.2105/AJPH.2017.303821.

Burnett, J., Jackson, S.L., Sinha, A.K., et al., 2016. Five-year all-cause mortality rates across five types of substantiated elder abuse occurring in the community. J. Elder Abuse Negl. 26 (2), 59–75. https://doi.org/10.1080/08946566.2016.1142920.

Charron-Chénier, R., Fink, J.J., Keister, L.A., 2017. Race and consumption: black and white disparities in household spending. Sociol Race Ethn. 3 (1), 50–67. https://doi.org/10.1177/2332649216647748.

Cohen, L.E., Felson, M., 1979. Social change and crime rate trends: a routine activity approach. Am. Soc. Rev. 44 (4), 588–608. https://doi.org/10.2307/2094589.

Cohen, L.E., Kluegel, J.R., Land, K.C., 1981. Social inequality and predatory criminal victimization: an exposition and test of a formal theory. Am. Soc. Rev. 46 (5), 505–524. https://doi.org/10.2307/2094935.

Dong, X., Simon, M.A., 2013. Elder abuse as a risk factor for hospitalization in older persons. JAMA Intern. Med. 173 (10), 911–917. https://doi.org/10.1001/jamainternmed.2013.238.

Federal Trade Commission, 2017. Consumer sentinel network data book for January–December 2016. Washington, DC: Federal Trade Commission.

Federal Trade Commission, 1998. Identity theft and assumption deterrence act. Washington, DC: Federal Trade Commission. https://www.ftc.gov/node/119459.

Ganzini, L., McFarland, B.H., Cutler, D., 1990. Prevalence of mental disorders after catastrophic financial loss. J. Nerv. Ment. Dis. 178 (11), 680–685. https://doi.org/10.1097/00005053-199011000-00002.

Golladay, K., Holtfreter, K., 2017. The consequences of identity theft victimization: an examination of emotional and physical health outcomes. Victims Offenders 12 (5), 741–760. https://doi.org/10.1080/15564886.2016.1177766.
Greenacre, M., Blasius, J., 2006. Multiple correspondence analysis and related methods. Chapman and Hall/CRC, Boca Raton, FL.
Greene, C., Stavins, J., 2016. Did the Target data breach change consumer assessments of payment card security? Research Data Report 16-1. Federal Reserve Bank of Boston, Boston, MA.
Harrell, E., 2015. Victims of identity theft, 2014. 1-26/NCJ 248991. U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, Washington, DC.
Harrell, E., 2019. Victims of identity theft, 2016. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. 1-29/NCJ 251147. https://www.bjs.gov/content/pub/pdf/vit16.pdf (last accessed 1.5.20).
Haushofer, J., Fehr, E., 2014. On the psychology of poverty. Science 344 (6186), 862–867. https://doi.org/10.1126/science.1232491.
Hindelang, M.J., Gottfredson, M.R., Garofalo, J., 1978. Victims of personal crime: an empirical foundation for a theory of personal victimization. Ballinger, Cambridge, MA.
Holtfreter, K., Reisig, M.D., Mears, D.P., Wolfe, S.E., 2014. Financial exploitation of the elderly in a consumer context. http://hdl.handle.net/20.500.11990/1235.
Holtfreter, K., Reisig, M.D., Pratt, T.C., Holtfreter, R.E., 2015. Risky remote purchasing and identity theft victimization among older Internet users. Psychol. Crime Law 21 (7), 681–698. https://doi.org/10.1080/1068316X.2015.1028545.
Inter-University Consortium for Political and Social Research, 2012. National crime victimization survey: identity theft supplement: codebook. University of Michigan, Ann Arbor, MI.
Inter-University Consortium for Political and Social Research, 2014. National crime victimization survey: identity theft supplement: codebook. University of Michigan, Ann Arbor, MI.
Koops, B.J., Leenes, R., 2006. Identity theft, identity fraud and/or identity-related crime. Datenschutz und Datensicherheit-DuD 30 (9), 553–556. https://doi.org/10.1007/s11623-006-0141-2.
McNeeley, S., 2015. Lifestyle-routine activities and crime events. J. Contemporary Criminal Justice 31 (1), 30–52. https://doi.org/10.1177/1043986214552607.
Miethe, T.D., Meier, R.F., 1990. Opportunity, choice, and criminal victimization: a test of a theoretical model. J. Res. Crime Delinquency 27 (3), 243–266. https://doi.org/10.1177/0022427890027003003.
Moore, T., Clayton, R., Anderson, R., 2009. The economics of online crime. J. Econ. Perspect. 23 (3), 3–20. https://doi.org/10.1257/jep.23.3.3.
Myers, J., Frieden, T.R., Bherwani, K.M., Henning, K.J., 2008. Ethics in public health research: privacy and public health at risk: public health confidentiality in the digital age. Am. J. Public Health 98 (5), 793–801. https://doi.org/10.2105/AJPH.2006.107706.
Olmstead, K., Smith, A., 2017. What the public knows about cybersecurity. Pew Res. Center.
Osgood, D.W., Wilson, J.K., O'malley, P.M., Bachman, J.G., Johnston, L.D., 1996. Routine activities and individual deviant behavior. Am. Soc. Rev. 61 (4), 635–655. https://doi.org/10.2307/2096397.
Pew Research Center. 2016. Millennials overtake baby boomers as America's largest generation. Pew Research Center. http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers/.
Pontell, H.N., 2009. Identity theft: bounded rationality, research, and policy. Criminol. Public Pol. 8 (2), 263–270. https://doi.org/10.1111/j.1745-9133.2009.00564.x.
Pratt, T.C., Holtfreter, K., Reisig, M.D., 2010. Routine online activity and internet fraud targeting: extending the generality of routine activity theory. J. Res. Crime Delinquency 47 (3), 267–296. https://doi.org/10.1177/0022427810365903.
Reyns, B.W., 2013. Online routines and identity theft victimization: further expanding routine activity theory beyond direct-contact offenses. J. Res. Crime Delinquency 50 (2), 216–238. https://doi.org/10.1177/0022427811425539.
Reyns, B.W., Henson, B., 2016. The thief with a thousand faces and the victim with none: identifying determinants for online identity theft victimization with routine activity theory. Int. J. Offender Th. 6 (10), 1119–1139. https://doi.org/10.1177/0306624X15572861.
Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., Hutton, S., 2004. Exploring the psychological and somatic impact of identity theft. J. Forensic Sci. 49 (1), 1–6. https://doi.org/10.1520/JFS2003178.
Titus, R.M., Heinzelmann, F., Boyle, J.M., 1995. Victimization of persons by fraud. Crime Delinquency 41 (1), 54–72. https://doi.org/10.1177/0011128795041001004.
U.S. Department of Justice [dataset], 2012. National crime victimization survey: identity theft supplement. Washington, DC: Office of Justice Programs, Bureau of Justice Statistics. ICPSR34735-v1. Doi:10.3886/ICPSR34735.v1. Retrieved from Inter-university Consortium for Political and Social Research: http://www.icpsr.umich.edu/icpsrweb/NACJD/studies/34735.
U.S. Department of Justice [dataset], 2014. National crime victimization survey: identity theft supplement. Washington, DC: Office of Justice Programs. Bureau of Justice Statistics. ICPSR36044-v1. Doi:10.3886/ICPSR36044.v1. Retrieved from Inter-university Consortium for Political and Social Research: http://www.icpsr.umich.edu/icpsrweb/NACJD/studies/36044.
Wartenberg, D., Thompson, W.D., 2010. Privacy versus public health: the impact of current confidentiality rules. Am. J. Public Health 100 (3), 407–412. https://doi.org/10.2105/AJPH.2009.166249.
Wilcox, P., Madensen, T.D., Tillyer, M.S., 2007. Guardianship in context: implications for burglary victimization risk and prevention. Criminology 45 (4), 771–803. https://doi.org/10.1111/j.1745-9125.2007.00094.x.
Williams, M.L., 2016;27;56(1):. Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. Br. J. Criminol. 21–48. https://doi.org/10.1093/bjc/azv011.