Understanding the effects of compromise and misuse of personal details on older people

Judy Watson
University of the Sunshine Coast
jwatson@usc.edu.au

David Lacey
University of the Sunshine Coast

Don Kerr
University of the Sunshine Coast

Paul Salmon
University of the Sunshine Coast

Natassia Goode
University of the Sunshine Coast

Abstract

An increasing number of older adults are being affected by scams that can lead to the compromise and misuse of their personal details. Previous research has investigated factors that increase the likelihood of falling victim to identity compromise and misuse; less is known about the non-financial impacts that result from the event or about the factors that influence these impacts. The aims of this study are to describe the identity compromise events experienced by older adults, and explore the non-financial impacts (i.e. behavioural, physiological, emotional and psychological), and external factors that might influence these impacts. The study used data collected by an identity compromise and misuse support service in Australia. The manner of compromise/misuse, the type and number of credentials involved, and the organisations/agencies that were contacted for advice following the event, were recorded. It was found that most events had an online element, were detected by the victim, and involved multiple identity credentials. Participants experienced a variety of behavioural, physiological, emotional and/or psychological impacts. More impacts were experienced where the event had an online element, where more credentials were compromised and where more points of contact were made to reach comprehensive advice. Misuse was not a contributory factor to the impacts experienced. Implications for further research are discussed.

Keywords: older adults; identity compromise and misuse; non-financial impacts; identity credentials; online

1 Introduction

Identity compromise and misuse continues to cause individuals financial and non-financial impact (Newman & McNally, 2005). Research has investigated strategies and methods for detecting identity compromise and misuse events, and has assessed the effectiveness of such approaches (Jenab & Moslehpour, 2016; Shah, Ahmed & Soomro, 2016). Researchers have explored the demographic factors (Anderson, 2006; Harrell, 2015) and personality traits (Holtfreter, Reisig, Pratt & Holtfreter, 2015) that increase the likelihood of succumbing to identity compromise. Society has sought to overcome the issue through technical and

educational solutions, and financial reimbursement of loss (Australian Payments Clearing Association, 2016).

Though important, financial reimbursement of the victim is not considered a holistic solution as the impacts of identity compromise and misuse are considerably wider, ranging from financial loss to physical, social, emotional and psychological issues (Benibo, Chambers & Thorne, 2016; Button, Lewis & Tapley, 2009a; 2009b; 2012; Cross, 2012; Golladay & Holtfreter, 2017; Identity Theft Resource Centre [ITRC], 2016; Sharp, Shreve-Neiger, Fremouw, Kane & Hutton, 2004). Although financial impacts may be relatively small, many victims experience impacts that negatively affect their general well-being (Attorney-General's Department [AGD], 2016). Physical, behavioural, emotional and psychological impacts may also vary in intensity; victims have reported a variety of levels of severity for each of these impacts (Button, Lewis & Tapley, 2009b). Understanding the impacts resulting from events where the amount of financial loss is not the overriding factor may provide the basis for researchers and practitioners to develop better tailored solutions.

As a society we are obliged to consider the well-being of an individual whose identity has been compromised and find means to address the non-financial impacts. Identity compromise and misuse has been found to corrode faith (Australian Crime Commission [ACC], 2013) and allow fear to permeate through an individual's life (Anderson, 2006) to a point where victims may experience years of emotional distress (Schmitz, 2008). Furthermore it compromises trust and reduces confidence in the internet (Australian Communications and Media Authority [ACMA], 2009), a medium which has been demonstrated to improve the quality of life and health and wellbeing of older adults (Hasan & Linger, 2016; Shillair, Rikard, Cotton & Tsai, 2015; Sum, Mathews, Pourghasem & Hughes, 2009). Additionally, if the faith that older people have in online transactions (both financial and non-financial) can be restored and extended, government and institutional services may save money with online solutions (Griffiths et al., 2017). This may enhance health and well-being through better interventions whilst providing significant savings for taxpayers and the nation. Therefore it is important to increase understanding of the antecedents of the impacts that victims' experience enabling the construction of better support frameworks to assist older adults to cope with an event. The aim of this study is to explore and understand the non-financial impacts of identity compromise and misuse, and the influences that might shape the impacts experienced by adults aged 65 years and older.

2 Background and Theoretical Basis

2.1 Identity Compromise and Misuse affecting older adults

It is recognised that the methods criminals use to achieve identity compromise are diverse and are constantly evolving (AGD, 2016).

Reports published in Australia and internationally show that increasing numbers of older adults are falling victim to identity compromise and misuse. For example, a survey undertaken in Australia in 2014/15 revealed that compared to 2010/11 more Australians, aged 55 and over, were exposed to at least one scam (57% and 33% respectively) (Australian Bureau of Statistics [ABS], 2016a). It was also reported that credit card fraud in this age group increased to an estimated four percent of the population (ABS, 2016a). In the UK, between 2014 and 2015, the number of identity compromise and misuse victims aged over 60 increased by 52 percent (Cifas, 2016). In the US, an increasing number of older adults are reported to be falling victim

to identity compromise and misuse; almost half a million more adults aged over 65, were victims of identity compromise and misuse in 2014 than in 2012 (Harrell, 2015). Although research has reported that some victims are able to overcome the experience and return to their normal life pattern relatively quickly (Benibo et al., 2016; Turville, Yearwood & Miller, 2010), others are devastated by the experience (Button, Lewis & Tapley, 2012a; ITRC, 2016; Cross, Richards & Smith, 2016) to the extent that there are a few reported cases of victims committing suicide (Cross, Smith & Richards, 2014).

2.2 Impacts of identity compromise on the wellbeing of the victim

Research has reported a range of physical impacts with detrimental consequences to health, such as insomnia, heart palpitations and loss of appetite (Cross et al., 2016; ITRC, 2016; Sharp et al., 2004). Previous studies report that the majority of the participants experience intense emotional and psychological impacts (ITRC, 2016) with participants describing that they had experienced a combination of emotions (Cross et al., 2016). The range of emotional and psychological impacts include but are not limited to anger, embarrassment, guilt, humiliation, paranoia, stress and worry (Cross et al., 2016; ITRC, 2016; Sharp et al., 2004). In turn, each of these emotional and psychological impacts may lead to further emotional states and behavioural actions as the victim attempts to cope with the circumstance they find themselves in (Cross et al., 2016).

Previously it has been reported that victims of online fraud change their behaviour (Smith & Hutchings, 2014; Turville et al., 2010) and may be less prepared to use online environments (Button et al., 2009a; Hille, Walsh, Brach & Dose, 2011). Other behavioural changes, such as becoming more cautious, have also been noted (ABS, 2016b; Button et al., 2009b). Though these impacts are varied it should be noted that the true range of impacts may not be understood as research acknowledges that victims do not always report to a central authority the fact that they have experienced identity fraud (Benibo et al., 2016; Smith, 2008). Further, what influences the impacts that individuals experience is unclear and there is no specific research on this with regard to older adults.

2.3 Theoretical basis

Technology Threat Avoidance Theory (TTAT) (Liang & Xue, 2009) suggests that when individuals perceive a malicious threat in information technology and believe that the threat is avoidable they are motivated to use problem focused coping measures. If they believe the threat is not completely avoidable emotion focused coping mechanisms will be initiated. TTAT proposes that threat perception is greater where perceived susceptibility to a threat and belief in the severity of the threat is increased. Furthermore the perception of threat is proposed as the motivating factor in commencing avoidance behaviour (Liang & Xue, 2009). Liang and Xue (2009) posit that threat avoidance is instigated with a coping appraisal process which has three antecedents; perceived effectiveness, perceived costs, and self-efficacy. TTAT proposes that these antecedents influence the perception of the avoidability of a threat. The theory suggests that where an information technology threat is apparent individuals will be motivated to protect themselves by undertaking a safeguarding action and/or performing emotion-focused coping. The adoption of a problem focussed coping strategy through the action of taking a safeguarding measure is more likely when an individual feels in control of the situation. Emotion focused coping strategies are more likely to be adopted where individuals feel they have less situational control (Liang & Xue, 2009). Indeed, coping theories such as Protection Motivation Theory (Rogers, 1975) and the Extended Parallel Process Model (Witte, 1992; Witte

& Allen, 2000) posit that emotional responses, such as fear, concern and anxiety, may be caused by threat and coping appraisals.

2.4 Hypotheses development

The perceived severity of a situation is seen as a critical determinant of protective behaviour (Boss, Galletta, Lowry, Moody & Polak, 2015; Witte, 1992). In a situation where an individual's identity has been compromised/misused, perceived severity has been seen as an individual's subjective assessment of the damage caused by the fraudulent use of that information (Li, Yazdanmehr, Wang & Rao, 2018). The environment in which an identity compromise and misuse event occurs may be a factor that influences that subjective assessment. Indeed, there are fundamental differences between identity compromise events that occur in online and offline environments. For example, individuals who experience identity compromise in an offline environment, such as the physical theft of a purse or wallet, may quickly become aware of the loss and therefore recognise the risk to their identity credentials. Where the event occurs online the individual may not know that a compromise has occurred for some period of time afterwards (Reyns & Randa, 2017) and in the case of romance scams they may be in denial that any compromise has occurred (Whitty & Buchanan, 2016). Additionally, in such cases the credentials that have been compromised may be unknown and difficult to assess adding another layer of complexity to the event and reducing the amount of control a victim has over the unfolding situation. It has been suggested that fear of the unknown may be a causal factor of anxiety and the tipping point for experiencing psychological response (Carleton, 2016). Any loss of control felt by an individual may make the difference between an individual adopting a problem focussed coping strategy and an emotion focussed coping strategy where more impacts are likely to be experienced. Therefore we hypothesise:

H1 - Events that have an online element will result in a greater number of impacts being experienced.

It has been reported that there are three main stages of identity compromise and misuse (Turville et al., 2010). Stage one represents the compromise event where a perpetrator acquires an individual's identity information, stage two is the misuse stage and stage three occurs when the individual becomes aware of the misuse of their identity (Turville et al., 2010). In some cases the misuse stage may be prevented through intervention, this may result in fear of the unknown being reduced or prevented. As a result individuals may feel more in control of the situation and hence more likely to adopt a problem focused coping strategy. Therefore we hypothesise:

H2 - Fewer impacts will be experienced where misuse of the compromised identity credentials has not occurred.

Previous research has acknowledged that there are many channels for reporting financial loss from fraud (Button, Tapley & Lewis. 2012b; Cross et al., 2016; Smith, 2008). Loss of identity credentials that do not necessarily have financial implications (e.g. passports and driving licences) have the potential to extend the number of organisations to which the event may need to be reported. This suggests that the greater the number of credentials compromised, the greater the number of organisations that an individual will have to contact to report the issue. Where more organisations have to be contacted it is likely that the time to resolve the issue will be increased. It has been found that the longer it takes a victim to resolve the issue the more likely it is that there will be more impacts of a greater intensity (Benibo et al., 2016; Harrell, 2015; Sharp et al., 2004), and the perceived severity of victimisation is impacted (Li et

al., 2018). Additionally the extent of misuse of personal information has been found to contribute to the self-assessment of severity of victimisation, which was positively correlated with perceived distress (Li et al., 2018). Furthermore, where more credentials are compromised individuals may feel an increased loss of control of their identity. Therefore, we hypothesise:

H3 - More impacts will be experienced where more credentials have been compromised.

In addition, we also examined whether older adults experience more impacts when they contact a greater number of organisations/agencies in order to reach comprehensive advice. A delay in accessing comprehensive advice may negatively affect feelings of situational control resulting in individuals being less likely to adopt a problem focused coping strategy. We hypothesise:

H4 - More impacts will be experienced when a greater number of points of contact are made to reach comprehensive advice.

By exploring these hypotheses this study will investigate whether there is a relationship between the level of the identity compromise/misuse event and the impacts experienced following the event in a sample of older adults.

3 Method

3.1 Research design

This study used pre-existing data collected by an identity compromise and misuse support service (IDS) from 354 older adults. The aim of the IDS is to support individuals from Australia and New Zealand that experience identity compromise and misuse (www.idcare.org). The IDS is a not-for-profit and registered charity. The study was formally approved, by exemption, by the human research ethics committee of the University of the Sunshine Coast.

3.2 Description of data source

The dataset was sourced from the call centre associated with the IDS. The data had been collected and logged by the IDS during telephone calls between the call centre case managers and the individuals who were searching for assistance.

The data was collected when an individual first made contact with the service. Given the nature of the IDS this means that data is collected at a point in time when the individual is still searching for assistance in overcoming the threat to their identity. The data used in this study represents one moment in time and it is important to note that the identity compromise/misuse event may have occurred at a considerably earlier time. Interviews vary in length depending on the nature of the identity compromise/misuse event and are tailored to support the individual. Prior to data collection, the IDS routinely seek, from all individuals, consent to use the data for research purposes.

The data was collected and recorded by experienced case managers, trained in psychology, who used semi-structured telephone interviews to gather information from older adults who contacted the IDS call centre for assistance over an eight month period. For this study older adults are defined as individuals aged 65 years or older.

The interview schedule, designed by the IDS, focussed on the 'journey' the individual had taken in reaching the IDS, other questions were designed to provide greater insight into the event itself (see Appendix 1). Data was recorded in the customer relationship management

(CRM) software KNACK, which is a customisable online database platform. Responses were notated into the CRM software at the time of the telephone call; responses to open ended questions were paraphrased using uniformity of language terminology within the IDS organisation.

To ensure anonymity, the interview process recorded very little demographic data other than gender, age range and whether or not the individual's first language was English.

Various questions (see Appendix 1) had predetermined categories of responses from which case managers selected an appropriate response, the predetermined responses were clearly defined resulting in negligible margin for error (see Appendix 2).

Individuals are also asked if they have experienced any impacts following the compromise of their identity, and case managers identify and record the individual's emotional and psychological response to the event (see Appendix 3) using adapted scales. The scales used to measure responses to questions regarding the behavioural, physiological, and emotional and psychological impacts that individuals experience were adapted from counselling theories and approaches. These include passive observations of depression and anxiety indicators including the Depression Anxiety Stress Scales (DASS) (Lovibond & Lovibond, 1995) and the State-Trait Anxiety Inventory (Balsamo et al., 2013). The details of the adapted scales can be found in Appendix 4.

3.3 Sample

All participants were 65 years of age or over; however the IDS does not record specific age data. To be included, participants had to be a resident of Australia and had at least one form of their identity information compromised. Following data collection, the dataset was examined for cases that related to those not resident in Australia (n = 70) and for cases where credential compromise did not occur (n = 12). A total of 82 cases were removed from the data set resulting in 272 Australian cases where at least one form of identity compromise had occurred.

The sample comprised 144 males (52.9%) and 127 females (46.7%). Gender was not recorded for one individual. English was the first language of 265 (97.4%) therefore only 7 (2.6%) were considered to be linguistically diverse.

3.4 Data analysis

The interview data was coded into the qualitative data software program, NVivo, allowing responses from open questions and those that did not follow the predetermined scheme to be coded accordingly. Organisational names nominated in response to other questions were analysed and classified into generic categories representing organisational sectors, for example financial institutions, telecommunication organisations etc.

Responses from questions regarding the behavioural, physiological, emotional and psychological impacts were analysed and coded to the following four categories by the first named author: behavioural impacts, physiological impacts, self-reported psychological impacts, and identified psychological and emotional impacts. Coding examples can be found in Table 1.

A second analyst undertook an inter-rater coding reliability test on the whole dataset, any differences in coding being resolved through discussion between the analysts. Based on the percentage of analytical agreement a reliability score of 80.6 percent was realised. The

reliability score was calculated by dividing the number of agreements by the total number of times coding was required. This is considered an appropriate way to determine reliability scores with qualitative data and a score above 80 percent is considered to be acceptable (Jentsch & Bowers, 2005).

Text coded	Type of impact
I do not really go on the internet for anything apart from searching for information, now I definitely won't I have always been vigilant, but now am more so.	Behavioural
Not sleeping Had a huge spike in blood pressure.	Physiological
I don't trust myself on the computer anymore I feel anxious and worried about what might happen with my details.	Self-reported psychological
Paranoid Distrusting	Identified psychological and emotional

Table 1: Coding examples

Descriptive statistics were used to describe the data.

Tests of normality indicated that the data was not normally distributed, therefore non-parametric tests were conducted. The Mann-Whitney U test was used to investigate H1 and H2. The Mann-Whitney U test is used to test differences between conditions where non-parametric data has been identified (Field, 2009).

To investigate H3 and H4 scatter plots were used to show relationships and trends within the data. To further explore the associations, bivariate correlations using Spearman's Rho were undertaken to identify any significance in the associations. Spearman's Rho is used to test for associations where non-parametric data is present (Field, 2009).

3.4.1 Dependent variables

The dependent variables represent self-reported impacts experienced by each participant and impacts identified by case managers. The self-reported impacts variable is a count variable constructed by summing the total number of behavioural, physiological and self-reported psychological impacts reported by participants. Likewise, the identified impacts variable is a count variable and again was constructed by summing the total number of emotional and psychological impacts identified by the case managers.

3.4.2 Predictor variables

The predictor variables represent the factors being investigated, Table 2 details the predictor variables and where each was sourced.

Dependent and predictor variables were coded and calculated by an analyst following which a second analyst undertook an inter-rater coding reliability test, as described in section 3.4, on 20 percent of the dataset. A reliability score of 97.5 percent was realised which was also considered to be acceptable.

Predictor variable	Source
Place of compromise/misuse (Online/Not online/Unknown)	Case notes; Compromise methods reported; Misuse methods reported
Compromise only or misuse occurred (Compromise only/Misuse)	Case notes; Compromise methods reported; Misuse methods reported; Whether attempted misuse of information was successful
Number of credentials compromised	Count variable calculated by summing the number of identity credentials the individual reported as being compromised
Number of points of contact to reach comprehensive advice	Count variable calculated by summing the people/organisations/agencies/sources that individuals reported they had connected with while searching for comprehensive advice

Table 2: Source of each predictor variable

4 Results

4.1 Compromise/Misuse event

The majority of compromise and/or misuse events (76.84%, n=272) contained an element of online activity, in other words either the compromise or the misuse or both occurred online (59.19%, n=161). A further 34.56 percent (n=94) of the events did not have an online element leaving 6.25 percent (n=17) of the participants not knowing how their identity credentials were compromised or misused.

Almost all participants (98.53%, n=268) nominated the way in which they were notified of the issue, the majority (76.10%, n=207) detected the compromise/misuse themselves. A further 7.72 percent (n=21) percent were alerted by family, friends or acquaintances, whilst financial institutions and other businesses/agencies each notified 5.88 percent (n=16) of the participants.

4.1.1 Compromise event

Almost 90 percent of the sample (89.97%, n=242) reported that at least one form of their personal identity credentials had been compromised. The remaining participants (11.03%, n=30) did not consider that their personal details had been compromised even though they reported being subject to events such as data breach incidents, remote access scams or household theft of personal papers.

Of those who were able to report where their credentials were compromised (n=177), almost half (n=79); reported various online situations whilst 55.37 percent (n=98) reported offline situations. Twenty four different sources of compromise were cited of which the top five were telephone phishing (33.90%, n=60), data breach (10.17%, n=18), email phishing (7.91%, n=14), website scams (6.21%, n=11) and household theft (5.65%, n=10).

4.1.2 Misuse event

Participants were asked if they believed their compromised credentials had been misused. Just over half (58.82%, n=160) reported no misuse, however 41.18 percent (n=112) believed misuse had occurred. Of those that believed misuse had occurred 55.36 percent (n=62) reported that the misuse of their information had been successful. A further 14.29 percent (n=16) did not know if the misuse had been successful or not.

Of those that believed misuse had occurred 70.54 percent (n=79) reported that they were aware of between one and six methods of misuse. On average, 1.67 methods of misuse were reported

(SD=1.08, n=79). The most common first reported method of misuse was accessing bank funds that did not involve superannuation (39.24%, n=31), followed by credit card fraud (24.05%, n=19) and tax return misuse (8.86%, n=7).

4.2 Credentials compromised

An average of 4.94 credentials were reported to be compromised (SD=3.35, n=234). Most commonly one or four credentials were compromised (15.07%, n=41).

The actual credentials reported as compromised were varied, 25 percent (n=68) reported their driving licence as compromised. Other credentials reported as compromised, that have high value to criminals (AGD, 2016), were passports (21.70%, n=59), credit cards (21.30%, n=58), tax file numbers (19.50%, n=53) and medical card numbers (11.00%, n=30).

4.3 Points of contact

Of those who could name the organisation they first contacted (n=161) most participants reported that they initially contacted a relevant financial institution (24.85%, n=40). State/territory police (19.88%, n=32) were the second most frequent initial point of contact followed by the Australian tax office (13.66%, n=22).

On average, participants reported that 2.93 points of contact were required to reach comprehensive advice about resuming control of their identity (SD=1.32, n=272). The majority (94.85%, n=258) made multiple points of contact.

4.4 Impacts

4.4.1 Overview

Almost three quarters of the participants (74.27%, n=202) self-reported or were identified (by a case manager) as experiencing at least one non-financial impact (behavioural, physiological, emotional and/or psychological). On average, participants who experienced an impact experienced just under three impacts (Mean = 2.86; SD = 2. 08, n=202). Almost a quarter of the participants (23.53%, n=64) experienced impacts of more than one type, reporting or being identified as experiencing a mixture of behavioural, physiological, emotional and psychological impacts.

4.4.2 Impacts reported by participants

Over a third of the participants (35.66%, n=97) reported experiencing at least one impact. Psychological impacts were the most common type of self-reported impact experienced (18.75%, n=51).

Self-reported psychological impacts

Of those that self-reported an impact over half of the participants (52.58%, n=51) reported at least one psychological impact. As shown in Table 3, the most frequently self-reported psychological impact was an awareness and concern that personal information was in the hands of others (25.49%, n=13).

Self-reported behavioural impacts

Of those that reported an impact, almost half 47.42 percent (n=46) described at least one behavioural impact. The most frequently reported behavioural impact was considering no longer using an online device (19.57%, n=9), as shown in Table 3.

Self-reported physiological impacts

Of those that self-reported an impact almost one third of the participants (30.93%, n=30) reported at least one physiological impact. As shown in Table 3, the most frequently reported physiological impact was a feeling of nausea (73.33%, n=22).

Impact type	Impact	% participants
Self-reported psychological impacts	Aware/concerned that information is in hands of others	25.49
	Worried about the future	19.61
	Stressed	17.65
	Feels reputation has been affected	11.76
	Feels isolated	7.84
	Other self-reported psychological impact	62.75
Behavioural impacts	Is considering no longer using online device	19.57
	Negative impact on relationships	15.22
	Closed affected accounts	13.04
	Stopped using online device	8.70
	Time off work	4.35
	Stopped online shopping	2.17
	Is considering no longer shopping online	2.17
	Other behavioural impact	47.83
Physiological impacts	Feels sick	73.33
	Trouble sleeping	40.00
	Trouble staying asleep	6.67
	Other physiological impact	3.33

Table 3: Most common self-reported impacts by impact type (multiple responses possible)

4.4.3 Impacts identified by case manager

Impacts were identified in 62.50 percent (n=170) of the participants. Emotional impacts were the most common type of identified impact with 58.82 percent of participants (n=160) being affected.

Emotional impacts identified by case manager

Over 90 percent of those identified by case managers as experiencing impacts (94.12%, n=160) were identified as experiencing at least one emotional impact. On average, these participants experienced 1.88 emotional impacts (SD=0.98, n=160). As shown in Table 4, the most frequently identified emotional impact was stupidity (26.25%, n=42),

Psychological impacts identified by case manager

Over 50 percent of those identified by case managers as experiencing impacts (51.18%, n=87) were identified as experiencing at least one psychological impact. On average, these participants experienced 1.33 psychological impacts (SD=0.68, n=87). As shown in Table 4, the most frequently identified psychological impact was being watchful and on guard (50.58%, n=44).

Impact type	Impact	% participants
Emotional impacts	Stupid	26.25
	Silly	18.13
	Vulnerable	16.25
	Anxious	16.25
	Embarrassed	15.00
	Foolish	14.38
	Distrusting	13.75
	Overwhelmed	13.13
	Regretful	12.50
	Violated	9.38
	Irritable	9.38
	Angry	9.38
	Deceived	6.25
	Helpless	5.63
	Paranoid	4.38
Psychological impacts	Watchful and on-guard	50.57
	No longer want to engage online	19.54
	Scared that they know where I live	12.64
	Have waves of strong feeling about it	11.49
	Trouble concentrating	8.05
	Other psychological impact identified by case manager	25.29

Table 4: Impacts most commonly identified by case manager (multiple responses possible)

4.5 H1 Events that have an online element will result in a greater number of impacts being experienced

A Mann-Whitney test indicated that the number of self-reported impacts was significantly greater when the compromise and/or misuse of personal information occurred in an online environment (*Mdn*=0, range = 0-7) rather than an offline environment (*Mdn*=0, range = 0-5); U = 6439.50, p = .01. However, a Mann-Whitney test indicated that the number of impacts identified by case manager was not significantly greater when the compromise and/or misuse of personal information occurred in an online environment (*Mdn*=1, range = 0-8) than an offline environment (*Mdn*=1, range = 0-7), U = 7002.50, p = .15.

4.6 H2 fewer impacts will be experienced where misuse of the compromised identity credentials has not occurred

A Mann-Whitney test indicated that the number of self-reported impacts was not significantly fewer when identity credentials were only compromised (*Mdn*=0, range = 0-5) than where misuse also occurred (*Mdn*=0, range = 0-7), U = 8939.50, p = .47. Similarly, a Mann-Whitney test indicated that the number of impacts identified by case manager was not fewer when only identity credentials were compromised (*Mdn*=1, range = 0-7) than where misuse also occurred (*Mdn*=1, range = 0-8), U = 8009.00, p = .06.

4.7 H3 more impacts will be experienced where more credentials have been compromised

As shown on the left hand side of Figure 1, there was a small to medium significant positive correlation between the number of credentials compromised and the number of self-reported impacts, r_s = .21, p <.01. As shown on the right hand side of Figure 1, there was also a small significant positive correlation between the number of credentials compromised and the number of impacts identified by case manager, r_s = .13, p =.03.

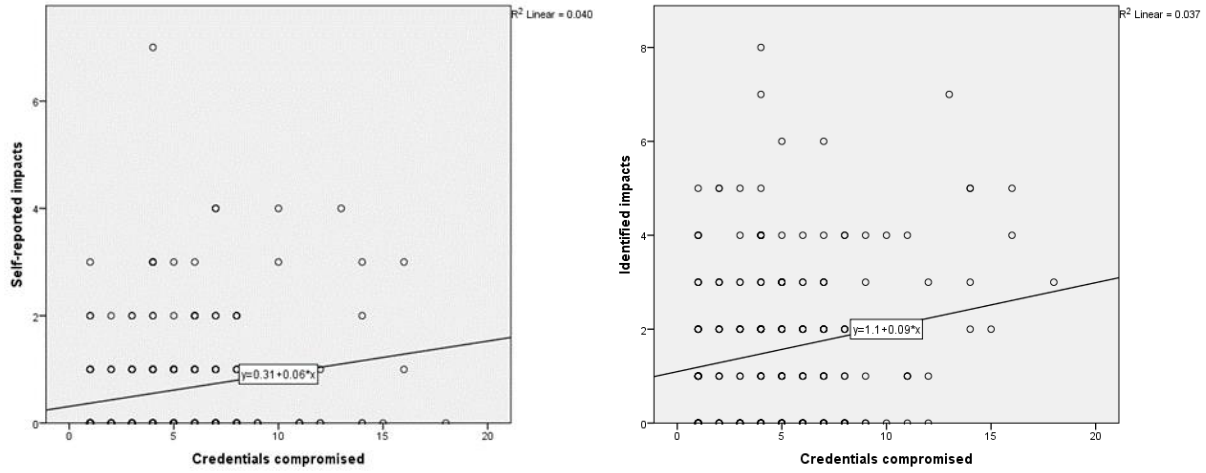

Figure 1: Scatter plot graphs for the relationships between the number of credentials compromised and the number of self-reported and identified impacts

4.8 H4 more impacts will be experienced when a greater number of points of contact are made to reach comprehensive advice

As shown on the left hand side of Figure 2, there was a small significant positive correlation between the number of points of contact to reach comprehensive advice and the number of self-reported impacts, $r_s = .16$, $p < .01$, the effect size was small. As shown on the right hand side of Figure 2, there was also a medium significant positive correlation between the number of points of contact and the number of impacts identified by case manager, $r_s = .37$, $p < .01$.

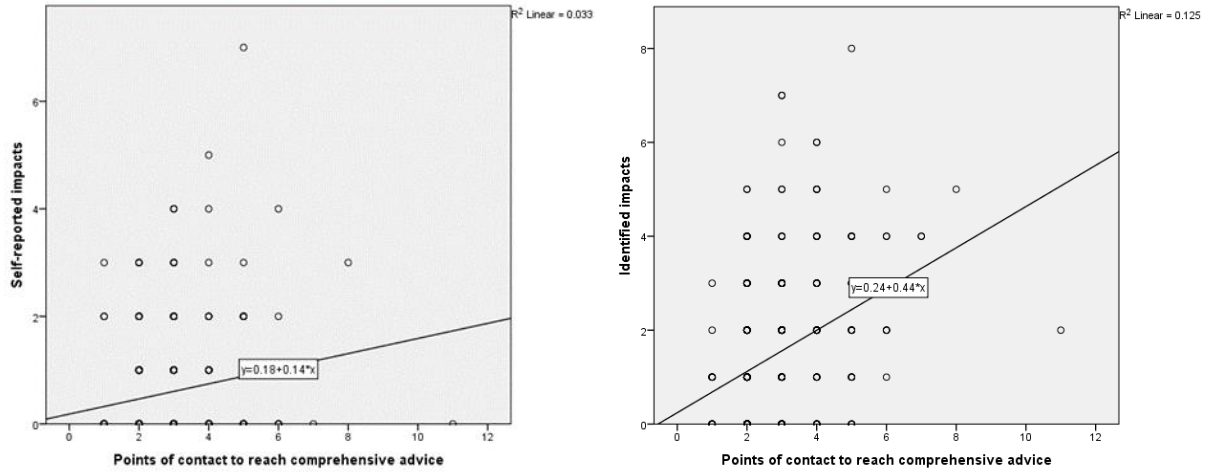

Figure 2: Scatter plot graphs for the relationship between the number of points of contacts made to reach comprehensive advice and the number of self-reported and identified impacts

5 Discussion

The aims of this study were to understand the impacts that older adults experience following identity compromise and misuse, and to build knowledge regarding the factors that influence them by testing the hypotheses detailed in section 2.4.

Approximately three quarters of the participants experienced at least one non-financial impact from falling victim to identity compromise/misuse; the greater percentage experienced more than one impact. Over one third of the participants were able to self-report a non-financial

impact, while two thirds were identified, by a case manager, as experiencing some form of this type of impact. Most detected the compromise and/or misuse of their credentials themselves and almost all connected with multiple points of contact to reach comprehensive advice. Not all knew how their credentials were compromised or misused however the majority involved an online element. Further the majority had multiple credentials compromised and at least one of the credentials was of high value, value being determined by financial worth in illegal online marketplaces (AGD, 2016).

The dataset provided evidence to support H1, the place of compromise and/or misuse (online) affected the number of self-reported impacts that were experienced. However there was no evidence to support H2, the added knowledge of misuse occurring did not increase the number of impacts experienced. A level of support was found for H3, suggesting that where a greater number of credentials are compromised more impacts will be experienced. Further, support was also found for H4 indicating that where more points of contact are made before reaching comprehensive advice more impacts will be experienced.

5.1 Main non-financial impacts

Undoubtedly older adults are impacted behaviourally, physiologically, emotionally and psychologically, and many but not all recognise the non-financial impacts they experience. In terms of frequency, emotional and psychological impacts dominated the experiences. Most commonly the experience left older adults more watchful and on-guard with participants being worried for the future and concerned that their personal information was in the hands of others. This suggests that they are aware that whether or not misuse has already occurred there is a potential that it could occur in the future. The reported physical impacts of feeling nauseous and experiencing sleep pattern disruption are likely to be the physiological manifestation of this worry and concern.

5.2 Behavioural change

Almost one third of those reporting a behavioural impact either considered stopping or had stopped using their online device. Further, no longer wanting to engage online was the second most identified psychological impact affecting almost 20 percent of the participants. This a concern when the drive is to move organisational contact methods to digital communication, and when research has reported that internet use can enhance older adults' quality of life and general well-being (Hasan & Linger 2016; Shillair et al., 2015; Sum et al., 2009).

5.3 Influential factors

Identity compromise and misuse events may be multifaceted with regard to many factors. These factors include place of compromise, place of misuse, methods of misuse, credentials involved, and knowledge of how to recover from the event. Notably, victims may not comprehend all of these factors. Research has reported that victims do not always know how compromise of their identity credentials occurs (Roberts, Indermaur & Spiranovic, 2013). In this study most participants were able to describe how their identity credentials were compromised and/or misused. For this dataset, the online element of the event was significantly related to participants experiencing a greater number of self-reported impacts. However, the fact that compromise had extended to misuse also occurring did not influence the number of impacts experienced.

This study has shown variance in the number of credentials compromised. Potentially, where more credentials are compromised, victims may feel greater confusion in knowing who to

contact and the reporting timescale may be extended by more organisations being involved. Prior research has identified that the amount of time spent resolving any financial impacts is directly related to amount of emotional distress and relationship issues encountered (Harrell, 2015). The results from this study indicate a link between the impacts experienced and both the number of credentials compromised, and the number of points of contact made to reach comprehensive advice.

5.4 The response journey

The response and recovery journey commences at the point of discovery. The study showed that on discovery the participants first contacted an array of different people, organisations or agencies. Financial institutions were the most common first point of contact; this may be because a victim's first thought is to secure their finances and prevent further loss, or because the credential compromised was issued by a financial institution. Other first points of contact include law enforcement agencies and organisations that issue credentials (e.g. passport office) or manage accounts (e.g. telco provider). Whatever the victims' intention, this study corroborates prior research that acknowledges a network of organisations involved in victims' response journeys (Button et al., 2012b; Cross et al., 2016), and in the identity ecosystem (Watson, Salmon, Lacey & Kerr, 2015). Research on fraud has shown that having many reporting channels leads to confusion in knowing who to report the crime to (Button et al., 2012b; Smith, 2008; UK Attorney General's Office, 2006). The people, organisations and agencies that older adults connect with before they reach comprehensive advice are an important link in the recovery process. Research has reported that following identity compromise and misuse, distrust commonly extends to almost everyone that the victim comes into contact with and this is exacerbated when it takes longer to restore their name (Benibo et al., 2016).

This study has provided confirmatory evidence in support of TTAT. Circumstances where emotional and psychological responses were heightened resulted from instances where there was less situational control. Furthermore, it was found that the theory applied in a context where users had already succumbed to a threat, identity compromise and misuse. Additionally, environmental factors (place, extent of event and length of response journey) have been found to influence the likelihood of users adopting emotional coping strategies, thereby building on TTAT. Future research should take into consideration the role that online environments, number of credentials compromised and length of response journey play in the post event experience of victims, and therefore in the likelihood of victims undertaking safeguarding actions or performing emotion-focused coping. Future research must consider the well-being of individuals whose identity has been compromised.

5.5 Future directions

More detailed understanding of the response network would develop greater knowledge of the response journey, highlight opportunities for feedback between stakeholders, and identify other individuals who provide support, such as social support, to the victim. Research has found that social support from family members results in less negative consequences for the victim (Golladay & Holtfreter, 2017). Greater understanding facilitates the opportunity to inform policy and practice, and thereby bolster support through better interventions.

This study has added to the knowledge-base by reporting on the impacts experienced by older adults and querying links between non-financial impacts and both the journey to seek

comprehensive advice, and the diversity of the identity compromise and misuse event. Future research should document the network of people, organisations and agencies that are involved in the response journey of older adults. Given the diversity of identity compromise and misuse events, investigation may be best served by undertaking case studies. Further research could extend across other demographic profiles.

5.6 Limitations

The study was limited by the small sample size. Additionally, due to further data limitations, it was not possible to compare results across different age groups. However, the findings are in line with previous multi-age group research which reports that impacts go beyond financial loss, and that there are many avenues for reporting an event. The data was also limited by the small percentage (11.7%) of the participants reporting any behavioural impact. This may be affected by the timing of the data collection as approximately two thirds of this study's cases were collected within seven days of the participant first becoming aware of the event. In that narrow time interval, participants may not have been conscious of behavioural impacts resulting from the event. Future research should investigate behavioural change at a later point in the response and recovery journey.

6 Conclusion

This study has increased knowledge around the identity compromise and misuse events that are experienced by older adults in Australia. The findings show that events are often diverse in occurrence and outcome. Many of the participants experienced non-financial impacts. These impacts were behavioural, physiological, emotional and/or psychological and it was not uncommon to experience multiple impacts. The findings suggest that when identity compromise and/or misuse occurs in an online environment older adults experience more impacts which may affect their behaviour. Furthermore, the actions that an older adult takes in responding to an identity compromise event appear to affect the non-financial impacts that are experienced. Finally the findings indicate that the number of credentials compromised matters as more impacts were experienced when more credentials were involved.

Acknowledgement

The authors would like to thank the reviewers for their helpful comments. Paul Salmon's contribution to this article and research programme is supported through an Australian Research Council Future Fellowship (FT140100681).

References

Anderson, K.B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing, 25,* 160–171. doi: 10.1509/jppm.25.2.160

Attorney-General's Department (AGD). (2016). *Identity crime and misuse in Australia 2016.* Retrieved from https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-crime-and-misuse-in-Australia-2016.pdf

Australian Bureau of Statistics (ABS). (2016a). *Personal fraud, 2014-15. In focus: Experiences of personal fraud for persons aged 55 and over (Cat no. 4528.0).* Retrieved from http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4528.0Main+Features172014-15?OpenDocument

Australian Bureau of Statistics (ABS). (2016b). *Personal fraud, 2014-15 (Cat no. 4528.0).* Retrieved from http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4528.0Main%20Features152014-15?opendocument&tabname=Summary&prodno=4528.0&issue=2014-15&num=&view=

Australian Communications and Media Authority (ACMA). (2009). *Australia in the Digital Economy, Report 1: Trust and Confidence.* Retrieved from http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf

Australian Crime Commission (ACC). (2013). *Identity Crime.* Retrieved from https://www.crimecommission.gov.au/sites/default/files/IDENTITY%20CRIME%20JULY%202013.pdf

Australian Payments Clearing Association. (2016). *Media release APCA releases interim payments fraud data.* Retrieved from http://www.apca.com.au/docs/default-source/2016-Media-Releases/apca-releases-interim-payments-fraud-data.pdf

Author (2015).

Balsamo, M., Romanelli, R., Innamorati, M., Ciccarese, G., Carlucci, L., & Saggino, A. (2013). The state-trait anxiety inventory: Shadows and lights on its construct validity. *Journal of Psychopathology and Behavioral Assessment*, *35*(4), 475-486. doi: 10.1007/s10862-013-9354-5

Benibo, B.R., Chambers, V., & Thorne, B. (2016). Breaking bad news to victims of identity theft: Lessons from medical doctors. *Journal of Accountancy, 222*(2), 30–34. Retrieved from https://www.journalofaccountancy.com/issues/2016/aug/giving-bad-news-to-identity-theft-victims.html

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly 39*(4): 837-864.

Button, M., Lewis, C., & Tapley, J. (2009a). *Fraud typologies and victims of fraud: Literature review.* London: National Fraud Authority. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118469/fraud-typologies.pdf

Button, M., Lewis, C., & Tapley, J. (2009b). *A better deal for fraud victims: research into victims' needs and experiences.* London: National Fraud Authority. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118468/better-deal-for-fraud-victims.pdf.

Button, M., Lewis, C., & Tapley, J. (2012a). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36–54. doi: 10.1057/sj.2012.11

Button, M., Tapley, J., & Lewis, C. (2012b). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. *Criminology and Criminal Justice, 13,* 37-61. doi: 10.1177/1748895812448085

Carleton, R.N. (2016). Into the unknown: A review and synthesis of contemporary models involving uncertainty. *Journal of Anxiety Disorders, 39*, 30–43. doi: 10.1016/j.janxdis.2016.02.007.

Cifas. (2016). *Criminals target UK youth as identity fraud rises.* Retrieved from https://www.cifas.org.uk/press_centre/criminals_target_UK_youth_as_dentity_fraud_rises

Cross, C. (2012). *The Donald Mackay Churchill Fellowship to study methods of preventing and supporting victims of online fraud.* Retrieved from: http://eprints.qut.edu.au/view/person/Cross,_Cassandra.html

Cross, C., Richards, K., & Smith, R.G. (2016). *The reporting experiences and support needs of victims of online fraud. Trends and issues in crime and criminal justice, No. 518.* Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi518.pdf

Cross, C., Smith, R.G., & Richards, K. (2014). *Challenges of responding to online fraud victimisation in Australia. Trends and issues in crime and criminal justice, No. 474*. Retrieved from http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi474.pdf

Field, A. (2009) *Discovering statistics using SPSS.* (3rd ed.) London: Sage Publications Ltd.

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimisation: An examination of emotional and physical health, *Victims & Offenders, 12,* 741-760. doi: 10.1080/15564886.20161177766

Griffiths, F., Bryce, C., Cave, J., Dritsaki, M., Fraser, J., Hamilton, K.,,…Sturt, J. (2017). Timely Digital Patient-Clinician Communication in Specialist Clinical Services for Young People: A Mixed-Methods Study (The LYNC Study), *Journal of Medical Internet Research, 19*(4), e102. doi: 10.2196/jmir.7154

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

Hasan, H., & Linger, H. (2016). Enhancing the wellbeing of the elderly: Social use of digital technologies in aged care. *Educational Gerontology, 42,* 749-757. doi:10.1080/03601277.2016.1205425.

Hille, P., Walsh, G., Brach, S., & Dose, D. (2011). Why online identity theft poses a major threat to e-business. *Proceedings of the ACM WebSci'11,* 1–2. Retrieved from: http://journal.webscience.org/518/1/207_paper.pdf.

Holtfreter, K., Reisig, M.D., Pratt, T.C., & Holtfreter, R.E. (2015). Risky remote purchasing and identity theft victimization among older internet users. *Psychology, Crime & Law, 21,* 681–698. doi: 10.1080/1068316X.2015.1028545

Identity Theft Resource Centre (ITRC). (2016). *Identity theft: The aftermath 2016.* Retrieved from http://www.idtheftcenter.org/images/page-docs/AftermathFinal_2016.pdf

Jenab, K. & Moslehpour, S. (2016). Cyber security management: A review. *Business Management Dynamics, 5*(11), 16–39. Retrieved from https://www.researchgate.net/profile/Kouroush_Jenab/publication/305220294_Cyber_Security_Management_A_Review/links/578510d408aef321de2a8f90.pdf

Jentsch, F., & Bowers, C. (2005). Team communication analysis. In N. A. Stanton, A. Hedge, K. Brookhuis, E. Salas, & H. Hendrick (Eds.), Handbook of human factors and ergonomics methods. Boca Raton, FL: CRC Press.

Li, Y., Yazdanmehr, A., Wang, J., & Rao, H.R. (2018). How Do You Cope: Individuals' Responses to Identity Theft Victimization. Paper presented at the Twenty-fourth Americas Conference on Information Systems, AMCIS 2018, New Orleans, LA, August 16-18.

Liang, H. & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly, 33*(1), pp.71–90. doi:10.2307/20650279.

Lovibond, P.F., & Lovibond, S.H. (1995). The structure of negative emotional states: Comparison of the Depression Anxiety Stress Scales (DASS) with the Beck Depression and Anxiety Inventories. *Behaviour Research and Therapy, 33,* 335-343. doi: 10.1016/0005-7967(94)00075-U

Newman, G.R. & McNally, M.M. (2005*). Identity theft literature review, National Institute of Justice Focus Group Meeting.* Retrieved from https://pdfs.semanticscholar.org/bb56/26ec1b5d31ff299c325a4bca93eee725de24.pdf.

Reyns, B.W., & Randa, R. (2017). Victim reporting behaviors following identity theft victimization: Results from the National Crime Victimization Survey. *Crime & Delinquency, 63,* 814–838. doi: 10.1177/0011128715620428

Roberts, L.D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law,* 20, 315-328. doi: 10.1080/13218719.2012.672275

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), pp.93–114. doi:10.1080/00223980.1975.9915803.

Schmitz, C. (2008). Identity theft victim claims emotional distress. *Inside Counsel,* (196), pp.65–66.

Shah, M.H., Ahmed, J. & Soomro, Z.A. (2016). Investigating the identity theft prevention strategies in m-commerce. *Proceedings of the International Conferences ITS, ICEduTech and STE,* 59–66. Retrieved from http://files.eric.ed.gov/fulltext/ED571576.pdf

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2004). Exploring the psychological and somatic impact of identity theft, *Journal of Forensic Sciences, 49,* 1-6. doi: 10.1520/JFS2003178.

Shillair, R., Rikard, R. V., Cotten, S.R., & Tsai, H-Y. S. (2015). Not so lonely surfers: Loneliness, social support, internet use and life satisfaction in older adults. *Proceedings of the iConference 2015.* Retrieved from http://hdl.handle.net/2142/73666

Smith, R.G. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change, 49,* 379-396. doi: 10.1007/s10611-008-9112-x

Smith, R.G., & Hutchings, A. (2014). Identity crime and misuse in Australia: Results of the 2013 online survey. Retrieved from http://www.aic.gov.au/media_library/publications/rpp/128/rpp128.pdf

Sum, S., Mathews, R.M., Pourghasem, M., & Hughes, I. (2009). Internet use as a predictor of sense of community in older people. *Cyberpsychology & Behavior, 12*(2): 235–239. doi:10.1089/cpb.2008.0150

Turville, K., Yearwood, J., & Miller, C. (2010). Understanding victims of identity theft: Preliminary insights. *Proceedings of the 2nd Cybercrime and Trustworthy Computing Workshop, CTC 2010,* 60–68. doi: 10.1109/CTC.2010.12

UK Attorney General's Office. (2006). *Fraud review: Final report.* Retrieved from: http://webarchive.nationalarchives.gov.uk/20070222120000/http://www.lslo.gov.uk/pdf/FraudReview.pdf

Whitty, M.T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims - both financial and non-financial. *Criminology and Criminal Justice, 16,* 176-194. doi: 10.1177/1748895815603773

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs, 59,* pp.329–349. doi:10.1080/03637759209376276

Witte, K. & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), pp.591–615. doi:10.1177/109019810002700506

Appendix 1

Interview questions

Questions
Do you believe your personal details have been compromised?
What do you believe was the method or source of your information being compromised?
What was the other source of compromise?
What credentials do you believe are compromised?
Which other credentials?
Do you believe there has also been misuse of your identification?
In what ways are you aware your compromised information has been misused?
What other way was information used?
Was the attempted misuse of your information successful?
In what way were you notified of the issue?
Notified by other?
Who did you first contact?
Other first contact
Have you already engaged another organisation for assistance with this matter?
Which organisation? #1
Is a 2nd Organisation already engaged?
2nd Org: Which organisation?
Is a 3rd Organisation already engaged?
3rd Org: Which organisation?
How did you find out about the IDS?
Which partner organisation?
Case notes (text about the individual's case)
Gender
State of residence
Age range
Linguistic diversity

Appendix 2

Questions with predetermined categories

Question	**Predetermined response**
What do you believe was the method or source of your information being compromised?	Cyber Stalking/Digital Stalking - known to me Cyber Stalking/Digital Stalking - not known to me Data Breach Email Face-to-face – known to me Job Application Lost Phishing – Email Phishing - SMS/Text Message Phishing – Telephone Remote Access Scam Social Media Telephone Theft - from household Theft - from letterbox Theft - from person Theft - from vehicle

Question	**Predetermined response**
	Unsolicited contact through mail
	Virus - malware/spyware
	Website - Competition/Survey
	Website – Job Application
	Website – Pop-up
	Website – Romance/Dating Scam
	Website – Travel Visa
	Website Scam
	Other
	Unknown
What credentials do you believe are compromised?	Address
	Australian Tax Office/Tax File Number
	Bank Account
	Centrelink
	Certificates - Birth/Death/Marriage
	Computer/Networking
	Credit/Debit Card
	Date of Birth
	Driver's Licence

Question	**Predetermined response**
	Email Address
	Full Name
	Insurance
	Login Info
	Medicare
	Mobile Phone
	MyGov
	Passport
	Phone
	Photos
	Superannuation
	Utilities Account Details
	Other
	Unknown
In what ways are you aware your compromised information has been misused?	Acquiring Personal Loan
	Bank – Access Funds (Not Super)
	Bank - New Account
	Credit Card
	Computer – Key-logger

Question	Predetermined response
	Computer – Malware/Virus
	Computer - Ransomware
	Damage Reputation
	Impersonate Email
	Impersonation on chat sites
	Manipulate Social Media
	Mobile Phone Account (including porting)
	Mobile Phone - New Account
	Obtain Investment Money/Shares
	Obtain Medical Benefits
	Obtain Debit Cards
	Open Online Account (email/social media/etc)
	Personal info passed to others
	Purchase Products
	Redirection of Mail
	Tax Return
	TFN used
	Transfer Funds
	Other

Question	**Predetermined response**
	None
In what way were you notified of the issue?	Another Business/Agency
	Australian Tax Office
	Bank or Financial Institution
	Credit Bureau
	Family member/Friend/Acquaintance
	Self-Detected
	Police
	Utility Organisation
	Other
How did you find out about the IDS?	Community outreach
	Friend/Acquaintance
	Media
	Partner organisation
	Web search
	Other

Appendix 3

Interview questions designed to identify impacts

Questions
In what way, if any, has your behaviour changed since this event?
In what other ways has this use of your information impacted you?
Psychosomatic effects – physical reactions
Emotional Impacts/Responses

Appendix 4

Scales used to measure responses (adapted from counselling theories and approaches)

Question	**Scale**
In what way, if any, has your behaviour changed since this event?	Affected reputation
	Closed affected accounts
	Is considering no longer shopping online
	Is considering no longer using online device
	Negative impact on relationships
	Stopped online shopping
	Stopped using online device
	Time off work
	Other
Psychosomatic effects – physical reactions	Aware have a lot of feelings about it, but don't want to deal with them
	Feel as if it hadn't happened or isn't real
	Feel sick
	Feeling numb about it
	Have dreams about it
	I think about it when I am not meaning to
	I try to remove it from my memory
	Jumpy and easily startled
	No longer want to engage online

	Other things keep making me think about it
	Pictures about it pop into my mind
	Scared that they know where I live
	Trouble concentrating
	Trouble sleeping
	Trouble staying asleep
	Try not to talk about it
	Try not to think about it
	Watchful and on-guard
	Waves of strong feeling about it
Emotional Impacts/Responses	Angry
	Anxious
	Deceived
	Distrusting
	Embarrassed
	Foolish
	Helpless
	Irritable
	Overwhelmed
	Paranoid

	Regretful
	Silly
	Stupid
	Violated
	Vulnerable

Copyright: © 2019 Watson, Lacey, Kerr, Salmon & Goode. This is an open-access article distributed under the terms of the Creative Commons Attribution-NonCommercial 3.0 Australia License, which permits non-commercial use, distribution, and reproduction in any medium, provided the original author and AJIS are credited.