Understanding Victim-enabled Identity Theft: Perpetrator and Victim Perspectives

David Lacey
Suzanne Barber
James Zaiss

UT CID Report #18-04

May 2018

This UT CID research was supported in part by the following organizations:
Understanding Victim-enabled Identity Theft
Perpetrator and Victim Perspectives

David Lacey
Centre for Human Factors & Sociotechnical Systems
University of the Sunshine Coast
Queensland, Australia
dlacey@usc.edu.au

Jim Zaiss and K. Suzanne Barber
Center for Identity
The University of Texas at Austin
Austin Texas USA
jim@identity.utexas.edu and sbarber@identity.utexas.edu

Abstract—Victim-enabled identity theft is a crime in which an individual victim is deceived into providing their personally identifying information (PII) to a criminal to facilitate its theft and/or misuse. In this paper we analyse a particular victim-enabled tax-related identity theft scheme recently reported in Australia, which has also been reported, in a slightly different guise, in the US. We find that this scheme, and others like it, are best understood when studied from both the perpetrator’s and the victim’s points of view. The criminal perspective and business practices have been captured and analysed in the Identity Threat Assessment and Prediction (ITAP) model developed by the Center for Identity at The University of Texas (UT CID). The victim perspective has been captured from multiple victim case files captured by IDCARE. The research findings support the view that combining perspectives enhances the analytical value of a threat assessment and prediction model. The multi-actor nature of victim-enabled identity theft complements the methodological approach adopted in the paper, and provides new insights on a growing form of identity theft that can inform future prevention and detection response strategies.

Keywords—identity theft; victimisation; telephone scams; iTunes; Personally Identifiable Information (PII)

I. INTRODUCTION

Our contemporary understanding of identity theft is influenced by popular views of mass data breaches, cyber intrusion and related hacking by state and non-state actors where the individual victim is portrayed as being almost a bystander. Little attention has been given to identity theft scenarios where the individual actually participates in the theft of their own identity. In such situations, the individual concerned actually enables the compromise of their identity and related credentials through directly facilitating its provision to the criminal, such as via phishing email or telephone scams. Victim-enabled identity theft is a relatively new concept [1]. Unlike indirect and arms length forms of identity compromise, such as via hacking or the physical theft of personally identifiable information (PII), victim-enabled identity theft is successful only when the individual concerned participates in the compromise of their own identity information through an action they have been deceived to perform. Victim-enabled identity theft covers the spectrum of deceptive practices that compromise PII from emails (i.e. phishing), SMS messaging (i.e. smishing), letter scams, and telephone scams where the channel of communication directly connects the criminal with the victim. The discerning feature of such crimes is that the victim themselves have volunteered their PII to the criminal under some deceptive pretext.

The very nature of such events results in multiple stakeholder actions. In any one event, there will be at least three actors: (1) the victim that has had their PII compromised; (2) the perpetrator who has deceived the victim into providing their PII; and (3) a third entity that has facilitated or enabled the misuse of the identity compromised, again often deceived into doing so by the criminal under the pretext that the criminal is the legitimate identity. The third entity in such cases can involve retailers, financial institutions, and telecommunications firms that provide goods and services to consumers on credit upon the presentation of an identity that is accepted as being legitimate and not stolen.

In some cases the actor network for victim-enabled identity theft can be large and complex. Not only does the initial theft and subsequent misuse of a stolen identity involve multiple actors, such as the criminal, the victim, and the organisation(s) that has issued the stolen PII, but networks expand as the victim seeks to respond to their identity theft experience and the criminal seeks to further misuse. Expanded response networks are networks of organisations, processes and technologies that victims engage to redress the initial compromise of their PII, the subsequent misuse event(s) that has been detected, and other actors and actions that can mitigate the risk of future misuse. These response networks include other actors, such as credit bureaus, the police, financial institutions, and other PII document issuing agencies, such as driver license issuers, that may be further targeted by the criminal to acquire additional PII to build the legitimacy of their newly acquired stolen identity. The expansion of the response network can add to a victim’s emotional and financial harm as they engage throughout this complex identity ecosystem. Unlike other crimes, the risk of experiencing further misuse of a stolen identity will endure for most victims of identity theft. It is a crime type where what is stolen is almost never returned, and where criminals can on-sell and trade stolen identities to other criminals for further misuse,
such as via illicit criminal marketplaces found within the dark net [2]. This places a great emphasis on victims to expand their response network to mitigate risks of future misuse of their PII.

This paper will explore victim-enabled identity theft from the perspective of both the victim and the criminal. The criminal perspective and business practices have been captured and analysed in the Identity Threat Assessment and Prediction (ITAP) model developed by the Center for Identity at The University of Texas (UT CID). The victim perspective has been captured from multiple victim case files captured by IDCARE. Bringing together both the victim and criminal perspective provides unprecedented insight into these types of victim-enabled crimes.

Additionally, this paper offers a detailed analysis of one such type of scenario, involving multiple actual cases, that has emerged as a growing challenge for Australia and New Zealand’s national identity and cyber support service, IDCARE. Investigating a specific scenario will provide both detailed insight as well as explain findings that both UT CID and IDCARE are uncovering in the larger investigations of identity theft and fraud.

II. VICTIM-ENABLED IDENTITY THEFT CASE ENVIRONMENT

This research study focused on events relating to the impersonation of the Australian Taxation Office (ATO) from telephone scammers who are deceiving Australians of their money under the pretext of an historical taxation debt. These cases represent the largest number of victims engaging with IDCARE [3]. The ATO, like most other national taxation authorities, administers tax laws as they apply to individuals and businesses that generate income or revenue. Australia has a taxation regime that requires individuals to submit annual taxation returns where they have earned a taxable income. Individuals may claim deductions against this taxable income where such deductions are admissible by law. The ATO may audit the accounts of individuals and, where discrepancies are identified, can direct individuals to repay tax and associated taxation interest if undeclared income or inappropriate deductions have been made. The ATO has historically written to individuals where such events occur to notify them of the outstanding taxation debt or related disputes involving their tax assessments.

This specific scam was first recorded by IDCARE in mid-2015. Media surrounding this specific case environment indicate that over 700 Australians have paid in excess of $1.7 million (AUD) to ATO telephone scammers since January 2015 [3]. The public reporting of this scam reveals that criminals are increasingly demanding iTunes gift cards as the preferred payment method to be employed by victims for settling their fictitious tax debt the criminal claims the victim owes the ATO. Failure to repay the tax debt immediately will result in arrest, according to the criminal [4]. The United States has seen similar such tax-related scams; the Treasury Inspector General for Tax Administration reports that between October 2013 and March 2016, victims collectively lost over $26.5 million (USD) to such scams.¹

In these scams the victim enables the compromise of their PII and is complicit in repaying the fictitious tax debt. In other words, these scams represent a victim-enabled identity theft.

III. IDENTITY THREAT ASSESSMENT AND PREVENTION MODEL: A PERPETRATOR PERSPECTIVE

The Identity Threat Assessment and Prevention (ITAP) model was developed at UT CID². The ITAP model is a structured, ever-growing, computational repository of information about incidents of identity theft, identity fraud, and data breaches in which PII is compromised. The raw data for the model are news stories, press releases, and government agency announcements concerning specific incidents or schemes in which PII is exposed, stolen, or misused. To date, the details of more than 5,000 incidents are represented in the ITAP model. The incidents span 16 critical infrastructure sectors, consistent with U.S. Department of Homeland Security infrastructure sector categorisation,³ and additional sectors to include consumer market sector, education and law enforcement.

The ITAP model is built and maintained using the AWAREness Suite™ software application. A wide variety of analytics – charts, graphs, other graphical displays, and reports – can be run on the ITAP modeled data to ascertain vulnerabilities, risks and consequences of these identity crimes [5].

In the ITAP model, each incident (i.e. identity theft, fraud or data breach case) is represented as a scenario describing the process or actions taken in carrying out the identity theft, fraud or data breach. These scenarios are complex occurrences consisting of a sequence of steps in the form of relatively simple, generic action-types or capabilities. Many other PII-relevant scenario attributes and relationships are represented in the model as well. The ITAP’s raw data currently comes exclusively from investigative news stories as well as government and law enforcement announcements (as opposed to, say, interviews with victims or reports from organisations that gather statistics about identity theft) and often captures an inclusive and exploratory description of the event. The ITAP model scheme is well suited for representing certain features of cases, such as entry vulnerabilities (how the crime was initiated) PII used/stolen/fabricated, victim demographics, actors, resources, consequences (financial, emotional and reputation) and market sectors impacted. Salient data captured in the ITAP model includes:

- The types or roles of the perpetrator(s), or performer(s), of the incident.
- The resources employed by the performer(s) to carry out the incident.

² https://identity.utexas.edu/
³ https://www.dhs.gov/critical-infrastructure-sectors
• The methods used – i.e. the steps undertaken – by the performers in carrying out the crime.
• The types of PII that were exposed, stolen, or misused in the course of the incident.

The ITAP model is comparatively sparse in details about the victims of these incidents. While it does capture various victim demographics (e.g. age group, income level, occupation, and citizenship) and some general information about an incident’s effects on the victims (e.g. levels of emotional stress and reputation damage), many details about the victims are rarely reported from the ITAP data sources and thus not added to the model. These include the specific emotions felt by the victim, the date when the victim first became aware of the crime, whether (and to whom) the victim reported the crime, secondary negative effects experienced by the victim, and many more.

In contrast, organisations – such as IDCARE – that counsel or assist victims of identity theft and fraud are bound to have much deeper information about the victims.

For this research study, an Australian victim-enabled identity theft scenario from April 2016 that several victims reported to IDCARE was selected for analysis. A media release on the scam was published on the ATO website in May 2016. The content of the media release was modeled as a scenario in ITAP. Then, the ITAP representation of the scam was compared to the victim-provided details gathered by IDCARE.

As reported on the ATO website, a scammer would telephone a perspective victim, claiming to represent the ATO and demanding payment of a tax debt in the form of an iTunes gift card. After a victim purchased a gift card, the scammer would convince the victim to read the card number over the phone. The scammer would then immediately sell or redeem the card. In many cases, the scammer would also succeed in convincing the victim to share PII, such as their tax file numbers, thereby opening up the possibility of further identity theft and fraud.

The scam was represented in the ITAP model as a scenario named ‘Australia: Phone Scammers Demand iTunes Gift Cards as Form of Tax Debt Payment’. (See Figure 1 below.) The sequence of steps (i.e. capabilities or generic action-types) assigned to the scenario, and their corresponding performers or actors, is as follows. (Note: The bracketed comments are added to aid the reader and are not part of the capabilities’ names. Such information is captured elsewhere in the ITAP as related to resources, PII, and consequences.)

Step 1. Communicate [via telephone]
   *Actor*: Telephone Scammer and Victim

Step 2. Impersonate [the ATO]
   *Actor*: Telephone Scammer

Step 3. Request [for PII of victim]
   *Actor*: Telephone Scammer

Step 4. Steal [PII of victim]

Step 5. Request [for payment via iTunes gift card]
   *Actor*: Telephone Scammer

Step 6. Purchase [iTunes gift card]
   *Actor*: Victim

Step 7. Acquire [iTunes gift card number]
   *Actor*: Telephone Scammer

Step 8. Sell [iTunes gift card number]
   *Actors*: Telephone Scammer and Gift Card Exchange Site

(Step 4, 5, 6, 7, and 8 are assigned as inputs to the scenario, as they are actions performed by the perpetrator to initiate the scam. Event-types 1, 2, 3, and 5 are assigned as outputs, as they are actions set in motion by the input actions.)

Event-types 1, 2, 3, and 5 are assigned as inputs to the scenario, as they are actions performed by the perpetrator to initiate the scam. Event-types 4, 6, 7, and 8 are assigned as outputs, as they are actions set in motion by the input actions.
the scenario while the other two were assigned as outputs. Thus, the first of these data-types was assigned as an input to the ITAP scenario. The resources assigned to the scenario are Telephone Scammer, Victim, and ITunes Gift Card. The performers and resources are shown in the fourth column in Figure 1. (See the third column in Figure 1.)

The types of PII involved in an incident are represented in ITAP as data-types that (along with event-types as discussed above) are assigned to the scenario as inputs or outputs. The ATO media release from which the present scenario was derived makes it clear that at least a Phone Number was needed to initiate the scam, and that the scammer got an iTunes Gift Card Number and, in some cases, a Tax File Number (and other PII which is not specified) from the victim. Thus, the first of these data-types was assigned as an input to the scenario while the other two were assigned as outputs.5 (See the third column in Figure 1.)

The ITAP model captures the criminal’s business process in each scenario as shown for the ATO case. The ITAP computational model allows for a single case to be analysed as well as a collective of scenarios with similar characteristics and trends. While the ITAP model highlights the criminal’s actions, capabilities, and consequences, the following section reviews the ATO case from victim’s perspective as seen by IDCARE victim services.

5 As will be apparent from the following section, IDCARE’s data on the ATO case includes additional details about the sorts of information exchanged beyond those mentioned in the media release. E.g., in some instances the scammer already had the victim’s full name and address and provided a fake ATO employee number; these were added as inputs to the ITAP scenario. Also, the scammers were sometimes able to get the victims to reveal their passport information; this was added to the outputs of the ITAP scenario.

IV. IDCARE CLIENT HARM ASSESSMENT & SUPPORT SERVICE: A VICTIM’S PERSPECTIVE

IDCARE’s primary mission is to reduce harm from identity and cyber-related threats to individuals impacted in the community. It operates Australia and New Zealand’s National Case Management Centre, which provides free counseling and pragmatic support to individuals that respond to instances where their PII has been put at risk in some way. Between January 2015 and July 2016, IDCARE invested over 3,500 hours in counseling individuals across Australia that experienced the specific ATO victim-enabled identity theft scenario in focus for this paper. IDCARE’s Case Management System records up to 114 variables in each case involving a specific client that engages its services. Clients provide IDCARE with permission to anonymously share their experiences for the purposes of furthering identity theft and cyber crime prevention and awareness research and initiatives. For the purposes of this paper, the experiences of fifteen clients have been extracted that align with the April 2016 period assessed by the ITAP. This section provides the victim perspective, in other words, the perspective from IDCARE clients captured during their engagement.

A. Victim Demographics

The majority of victims were male, aged between 25 and 45 years, and resided in metropolitan areas (approximately 60%). The spread of victims, even for a small sample, resided in all but two Australian states and territories. This is not an unusual finding given the channel used by the criminals to commit the crime was telephone, and therefore the criminal is not constrained geographically within Australia. Interestingly, two of the victims engaging IDCARE had English as a second language – this is approximately double the normal IDCARE victim demographic trend and may indicate the need for future research in exploring the vulnerability of those involving such scams where English is not a primary language.

B. Victim Insights of the Perpetrator

It was revealed in a number of cases that the criminal claimed that an audit had occurred for the years 2009 to 2013, resulting in a tax debt. Common tax debt values demanded by criminals from victims were: $15,000 (AUD), $10,000 (AUD), $4,848 (AUD) and $4,000 (AUD). The most common value demanded by criminals was $10,000 (AUD) – represented in four of the fifteen cases. In one instance a client remarked that they concluded it was a scam only when the criminal demanded a second payment after the client had paid the alleged tax debt.

One victim alleged that they attempted to validate the legitimacy of the message left by the criminal, but because they called on a weekend, the ATO’s telephone line was not in business hours. Analysis of what days of the week were preferred by criminals to make calls to victims indicates that they were active on every day of the week except Sunday.
Thursdays and Fridays appeared the most popular days for the criminals in making calls (six of the fifteen victims).

The scare tactics used by criminals included legitimising their role by providing their fictitious ATO employee number, by indicating to victims that there had been several previous attempts to inform them of the debt via letter and telephone, and by providing the victim’s full name and address.

Legitimising actions used by the criminals also mimicked legitimate messaging employed by the ATO. For example, in a number of cases, victims revealed that when telephone messages were left, the criminal would indicate that the victim had to return their call by a certain date and that they “should have their Tax File Number (TFN) handy”. The latter is a common message provided by the legitimate ATO as a means for individuals to confirm their identity when they call the real organisation.

C. PII Compromise and Further Criminal Exploitation

Twelve of the fifteen victims experienced the compromise of PII. In these situations, the scammer was not only successful in convincing the victim that they were the ATO, but they also convinced the victim to disclose their PII. On average, four different types of PII were obtained by perpetrators, including driver license, passport, and bank account information. Instances where such PII were targeted, the risk to victims of experiencing future direct misuse of such PII were heightened. IDCARE assesses each case that is presented to its National Case Management Centre as to the likelihood that the instance of compromise or misuse experienced by a victim will result in future direct misuse – in other words, the likelihood that the criminal does not need any other information about the victim to be able to keep misusing their PII. Nine of the fifteen victims that engaged IDCARE during the month of April on this specific victim-enabled identity theft scenario were assessed to have a medium to high risk of future misuse. Two clients had already experienced subsequent misuse by the time they had engaged IDCARE following the initial scam. Both misuse events were unauthorised access to the victim’s bank account and the subsequent withdrawal of money ($10,000 AUD and $4,000 AUD respectively). These experiences highlight the disassociation scams have from traditional forms of identity theft. While these cases represent a telephone scam, the risks of future identity theft remain where PII information is disclosed to the criminal. IDCARE experiences similar identity misuse occurring in relation to romance and job scams, as well as more traditional identity theft events, such as the physical theft of driver licenses and passports. According to the data in ITAP, stolen driver’s licenses and passports in the U.S are associated with losses totaling millions of dollars in the context of the approximately 5000 cases modeled.

E. The Biospsychosocial Impacts to the Victim

IDCARE is resourced with Identity Security Counselors. Their specialist staff are qualified counselors, psychologists and social workers that are trained in identity and cyber security in order to resource its National Case Management Centre. Their expertise is critical in working with individuals who are emotionally heightened and require practical and behavioural support to respond to the event experienced. Biological and psychological affects captured within the case group by the Counselors were varied. The most common included nausea, inability to concentrate, heightened stress and anxiety, and feeling physically unsafe (where residential address information was compromised).

D. Victim Insights on Why the Scam Works

IDCARE collects insights from victims on what made scams believable for them and what were the trigger points that made them ultimately convinced it was a scam. Most victims said they were initially convinced the scam was legitimate because the caller “sounded official”, they “felt scared of what would happen if [they] didn’t comply”, and the caller “had details about” them. The combination of these three elements featured in more than half of the clients’ reflections as to why they believed the criminal that they were the ATO.

The trigger point for most clients (9 of 15) that reshaped their view of the scenario from one of legitimacy to one of a scam mostly related to the excessive nature of the coercion applied by the scammer, the behaviour of the criminal not being consistent with Government practice (for example, payment via iTunes gift cards), and the accent of the criminal different to what they would expect to hear (a very heavy accent from the subcontinent). Victims also revealed having a general “gut feeling” or “suspicion” throughout the ordeal. In IDCARE’s experience victims of scams often reflect having a degree of suspicion throughout their engagement with scammers but only become convinced of the scam the moment they act upon the criminal’s demands [3].
F. Identity Ecosystem Journey for Victims

A key element of the IDCARE support process is to provide victims with detailed advice on the precise steps required to address the current event as well as mitigate the risk of future identity misuse. In other words, IDCARE provides victims with detailed information about the victims response network. IDCARE refers to these services as their Response Plans. On average, a response plan will inform a victim on the method of engaging with a relevant actor within the identity ecosystem, the nature of the engagement, the needs from the organisation, and likely timeframes and general standard of performance the victim can expect. The identity ecosystem includes the actors, individuals, and organisations that are dependent on working together and sharing information to protect and respond to related identity threats as part of the response network to a specific identity theft scenario [6].

IDCARE has a library of over a thousand separate response plans spanning more than 300 identity ecosystem actors. IDCARE tests these responses, with something akin to a “secret shopper” test, at least five times every quarter to ensure their clients receive the most accurate advice and guidance required across a multitude of different identity and cyber crime threat scenarios. For the victims of the scenario in focus, IDCARE estimates that they will need to initiate at least 11.92 engagements throughout the identity ecosystem based on the steps and pathways observed in each response plan they provided to these victims. Two of the fifteen clients had already estimated that they had spent between six and ten hours on the initial stages of response effort to protect their identity from future misuse.

V. ANALYSIS & CONCLUSIONS

This paper reveals that a rich picture of victim-enabled identity theft is achievable where the perpetrator and victim perspectives are presented. The ATO case shares some significant features commonly found among the roughly 5,000 scenarios in ITAP across multiple market sectors. For example, as shown in Figure 2 below, the ATO scammers stole or misused three of ITAP’s top four most commonly compromised types of PII: Name (36% of cases), Date of Birth (14%), and Address (14%). And Figure 3 reveals that the non-digital nature of the ATO scam is shared with the majority (53%) of ITAP scenarios. Furthermore, the ATO scenario’s step (i.e. constituent action type) Impersonate is found in about 700, or 14%, of all scenarios in ITAP.

To best understand what happened in the commission of identity theft and fraud, it is typically sufficient to model the criminal business process as seen in the ITAP computation model. However, there are a subset of cases, termed victim-enabled identity theft in this research, that require the modeling and inclusion of both the criminal and victim to fully capture and understand the commission of these crimes. Additionally, the full impact of these crimes is not fully understood without studying the victim response (as done by IDCARE) and a full appreciation of the longer-term impact of shared PII. Both IDCARE and UT CID have explored the elevated risks from released PII.
ITAP and IDCARE analysis pointed to the harvesting by criminals of multiple forms of PII. IDCARE assessed the majority of their cases as being a medium to high-risk event. In other words, for every person that has their identity stolen in this scenario, their remained an enduring risk that they could experience a further identity misuse based solely on the nature of the PII stolen. Victims enabled the provision of four separate PII credentials on average during the scam event. This represents four credentials within the ecosystem that have their integrity threatened and subsequent trust surrounding the legitimacy of their future usage jeopardised. In fact two of the fifteen cases examined by IDCARE observed an immediate subsequent misuse involving the unauthorised withdrawal of money from the victims’ bank account.

Finally, it should be noted that there is another perspective, besides those of the perpetrator and the victim, importantly involved in many cases of identity theft: that of the organisation(s) affected. Roughly one quarter of the scenarios in the ITAP model have an organisation or organisation type as one of their actors. Although the ATO is not itself a direct participant in the case under analysis here, its U.S. counterpart the Internal Revenue Service is an actor in many tax fraud scenarios in ITAP. Our understanding of these sorts of cases could undoubtedly be further enriched if we were to include organisation-provided data among our sources.

ACKNOWLEDGMENT

The authors wish to thank the Center for Identity Strategic Partners (https://identity.utexas.edu/strategic-partners) for their support of this research endeavor and IDCARE for the provision of case information. Dr David Lacey (co-author) is also the Managing Director and board member of IDCARE.

REFERENCES
