Identity theft and Australian telecommunications:

Understanding the risks for consumers

Australian National University

Identity theft and Australian telecommunications: Understanding the risks for consumers

Intervention evaluation and outcomes

David Lacey

June 2017

Identity theft and Australian telecommunications: Understanding the risks for consumers

Authored by **David Lacey**

Published in **2017**

The operation of the Australian Communications Consumer Action Network is made possible by funding provided by the Commonwealth of Australia under section 593 of the *Telecommunications Act 1997*. This funding is recovered from charges on telecommunications carriers.

University of the Sunshine Coast
Website: http://www.usc.edu.au
Email: kamurphy@usc.edu.au
Tel: +61 7 5459 4409

IDCARE
Website: http://www.idcare.org
Email: contact@idcare.org
Tel: 1300 432 273

Australian National University

Website: www.anu.edu.au

Email: sigi.goode@anu.edu.au

Telephone: +61 2 6125 5048

Australian Communications Consumer Action Network
Website: www.accan.org.au
Email: grants@accan.org.au
Telephone: +61 2 9288 4000
If you are deaf, or have a hearing or speech impairment, contact us through the National Relay Service: www.relayservice.gov.au

ISBN: 978-1-921974-52-6
Cover image: Design by Richard Van Der Male with image from Shutterstock

This work can be cited as: Lacey, David (2017) 'Identity theft and Australian telecommunications: Understanding the risks for consumers', Australian Communications Consumer Action Network, Sydney.

Table of Contents

Figures and Tables ii

Acknowledgements 1

Introduction 2

Intervention 1: Building the threat and exploitation picture 3

- Introduction 3
- Approach 3
- Results and analysis 4

Intervention 2: Examining consumer experience pathways and impacts 8

- Introduction 8
- Approach 9
- Results and analysis 10
- Intervention responses 14

Conclusions 16

Appendix 18

Authors 20

Figures and Tables

Figure 1: Service providers of the telephone number used by scammers 5

Table 1 Scam type by Allocatee and Service Provider 6

Figure 2 Unauthorised mobile porting event.. 9

Table 2 Client response satisfaction score by market segment... 11

Acknowledgements

IDCARE would like to thank ACCAN, ANU and USC for allowing its information and data to be used to inform stakeholders about the current risks and experiences of consumers when confronting complex communication-enabled identity theft events.

Introduction

The research team developed two interventions informed from the analysis of approximately 4,000 IDCARE case files. The interventions focused upon examining the following gaps in knowledge:

1. How criminals exploit and intersect with telecommunications providers domestically to achieve their ends
2. What happens to consumers, following specific telecommunications-enabled identity theft events

This report presents the results of these interventions.

It was obvious from earlier analysis[1] that scams exploiting telecommunications channels were the dominant method of compromising IDCARE clients' identity. Yet few insights could be provided regarding the degree to which actors across the information and communications technology (ICT) marketplace were facilitating such compromise events, knowingly or unknowingly, and whether such knowledge could assist in building new resilience and response measures by telecommunications providers, IDCARE and consumers.

Previous work in this project highlighted the unique complexities of the response environment confronting consumers. IDCARE's services assist individuals in understanding how to respond to identity theft events and mitigate future risks. Not much is known about how an individual responds to identify theft and, in particular, to complex identity theft events where compromise and misuse actions have occurred. Unauthorised mobile phone porting is a complex event that requires consumers to engage widely across the telecommunications ecosystem to repair and recover from their compromised identity. The first intervention detailed in this report addresses this issue.

The second intervention aimed to address the knowledge-gap in the post-IDCARE engagement journey for telecommunications consumers confronting complex events. The re-engagement of these clients by IDCARE directly assisted in understanding whether expectations and response requirements across the ecosystem were met, the feeling consumers had towards ecosystem engagement points, and specific consumer needs when confronted with a response journey.

[1] See the two earlier reports from this project: *Identity theft and Australian telecommunications: A structured literature review*; and *Identity theft and Australian telecommunications: Case analysis*. Both available from the ACCAN web site.

Intervention 1: Building the threat and exploitation picture

Introduction

Telephone scams are the most prominent form of identity compromise reported to IDCARE by its clients since the organisation commenced operations in October 2014. This intervention sought to examine the attributes of these scams. Specifically, this intervention relied upon clients reporting to IDCARE the telephone numbers used by scammers, either through caller ID information or through voluntary disclosure by the scammers themselves. The latter method of collection is often relevant for scammers who impersonate organisations and leave messages on landlines asking for individuals to call them back.

Approach

From 1 January 2017 to 31 March 2017, IDCARE engaged 555 clients a total of 1,236 times following their direct interaction with telephone scammers. IDCARE staff sought each client's consent to share details they obtained about the scammers for the purposes of research, prevention and awareness raising. This was conducted in accordance with ethics approval from the University of the Sunshine Coast (A/17/918).

Attributes collected included:

- the telephone number(s) scammers called from
- the telephone number scammers asked individuals to make future calls to
- the organisation the scammer was purporting to be calling from
- time and date of engagement
- postcode, age range, gender and whether English was a second language of the person who received the call(s)

On receipt of the landline telephone number from Australian clients, IDCARE used a tool[2] to determine the 'allocatee' of the number and the 'service provider'.

The Australian Communications & Media Authority (ACMA) defines the 'allocatee' as the organisation that has purchased the spectrum of numbers available via ACMA's wholesale number distribution service. The 'service provider' is the organisation that actually sells the allocated number. In other words, the 'service provider' is the organisation that would have a direct engagement with the scammer or a third party that has, in turn, sold the service to the scammer.

The data collection was not able to determine whether the 'service provider' had subsequently on-sold the service to a third-party and, as such, whether this third-party is the one with the

[2] https://www.thenumberingsystem.com.au

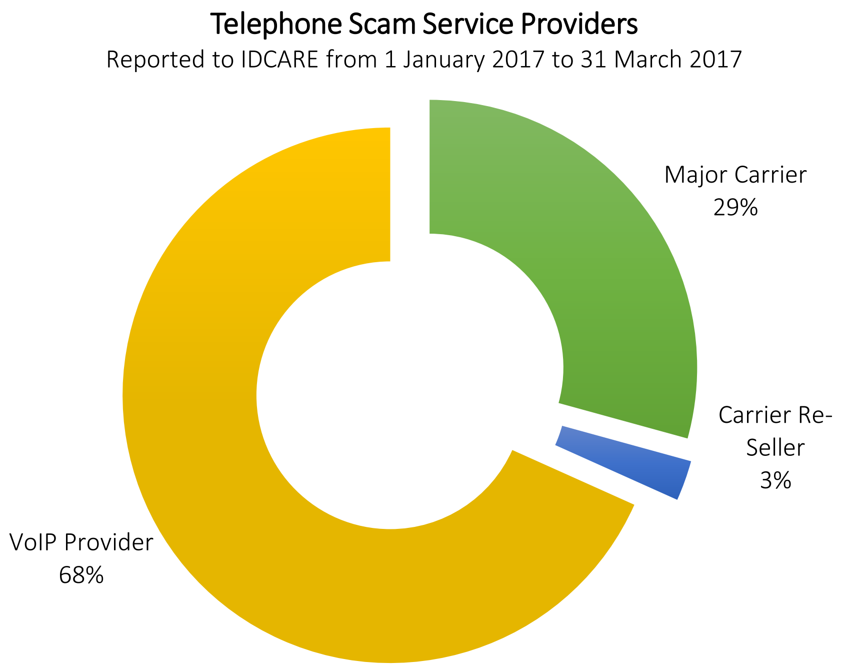
direct customer relationship with the scammer. However, the 'service provider' is legally responsible for that recorded relationship. It is also important to note that the 'allocatee' and the 'service provider' may be the same organisation. Where they are not the same, the 'service provider' may lawfully sell the number allocated to another entity in legal, regulated on-selling arrangements.

Results and analysis

Approximately 61 per cent of the clients studied were aged 25 to 65 years, 58 per cent were female and 3.4 per cent spoke English as their second language. There was a slightly higher percentage of metropolitan residents among this cohort when compared with non-telephone scam clients engaging IDCARE over the same period (59.5 per cent compared with 55.2 per cent of residents). This result signals a slightly higher median weekly household income for telephone scam clients (ABS: 2011). It is not clear from this analysis whether affluent Australians are being specifically targeted by telephone scammers based on a comparison of residential postcodes, however it may offer some explanation for the increased representation. Another explanation may relate to the more accessible nature of third parties – such as international fund transfer services and iTunes gift voucher sellers – with which scammers target individuals.

A total of 41 unique telephone numbers were provided by 38 per cent of these clients. The remaining 62 per cent of clients were not able to provide IDCARE with this information. Of these 41 telephone numbers, 21 were listed as having the same 'allocatee' and 'service provider' (nine of these were major carriers). Data collection of 'service provider' details enabled IDCARE to examine the preferences of scammers to engage particular industry groupings. For the purposes of this analysis, IDCARE divided 'service providers' into three groupings: Major Carrier (Telstra, Optus and Vodafone), Carrier Re-Seller (such as wholly or partly owned companies operated on the major carrier networks e.g. Virgin Mobile and Primus), and VoIP Provider (Voice Over Internet Protocol). The VoIP Provider category is restricted to companies that offer VoIP-only services, rather than including Major Carriers or Carrier Re-Sellers that offer VoIP products and services as well as other service delivery options.

Figure 1: Service providers of the telephone number used by scammers



The telephone numbers captured relate to telephone scams involving 14 brands in total. Of these, 11 were legitimate business and government brand names and three were fictitious. A little over two-thirds (68 per cent) of the telephone numbers scammers used were provided by specialist VoIP service providers, with the remaining third provided by major carriers and those operating from the carrier networks.

It is not possible to directly comment upon the preference towards VoIP providers from a criminal perspective; however a number of unique attributes may influence criminal preferences. For example, VoIP providers advertise services that conceal the true origin of account owners and call originators through offering ‘local numbers’. For a scammer this is critical, particularly in relation to the real-name brands exploited by scammers captured in the data holdings. The success of deception, particularly when a scammer impersonates an Australian government agency is likely to depend on whether the targeted individual believes the initiator of the call comes from within Australia. Australian government agencies prefer not to use offshore call centres, unlike their private sector counterparts that are also targeted by scammers.

In scams involving fictitious organisations (such as those alleging involvement of the ‘Australian Grants Commission’ and the ‘Accident Insurance Commission’) scammers used VoIP providers exclusively. There is also a slightly higher preference for scammers in these scenarios to call individuals to gain remote access to their devices in order to harvest credentials, banking details and/or leave ransomware on the accessed device. In such cases the scammers relied upon real name ‘ICT service providers’ such as Microsoft, Apple, Telstra and Norton to gain remote access to the receiver’s device on the pretext of a virus or compromised system requiring urgent attention.

In these cases, 72 per cent of scammers relied upon VoIP providers as their service provider compared with 68 per cent of all telephone scams where the scammer’s number was provided. This was the major scam category captured during the period (25 of 41 numbers captured were ‘remote access scam’ events).

Table 1 below lists the scam categories – i.e. the organisations the scammers are purporting to impersonate. Five categories were identified in the case information analysed by IDCARE:

1. Government: actual commonwealth, state or territory government agencies (such as the Department of Human Services, the Commonwealth Department of Public Prosecutions and the Australian Taxation Office)
2. ICT: actual information, communication and technology companies, including majors such as Telstra, Optus, Apple, Microsoft and Norton
3. Fictitious: names invented by the scammer (such as the ‘Australian Grants Commission’ and the ‘Accident Investigations Agency’)
4. Financial services: actual financial institutions, such as banks
5. Utilities: as distinct from telecommunications providers, this category captured real-name energy providers such as Energy Australia, AGL and Energex.

The use of fictitious entity names was less common than the use of real company or government agency names (only 17 per cent of cases where the telephone number was provided, and 16 per cent of all telephone scams).

Table 1 Scam type by Allocatee and Service Provider

	Allocatee			Service Provider		
	Major Carrier	**Carrier Reseller**	**VoIP Provider**	**Major Carrier**	**Carrier Reseller**	**VoIP Provider**
Government	2	1	4	2	1	4
ICT	7	1	17	7	0	18
Fictitious	0	0	7	0	0	7
Financial Services	1	0	0	1	0	0
Utilities	1	0	0	1	0	0
Total	**11**	**2**	**28**	**11**	**1**	**29**

Interestingly, scammers also relied upon major carriers more when impersonating real government agencies (such as the Australian Taxation Office and the Department of Human Services). While only a small sample of government numbers were obtained by clients (seven in total), almost half of all numbers reported for these scams were not allocated and provided by VoIP providers. This may mean that remote access scammers (those targeting a victim’s ICT devices) are different to those impersonating government agencies. This may be due to the differing requisite knowledge for these two types of scams.

Intervention 2: Examining consumer experience pathways and impacts

Introduction

Individuals that experience identity and cyber-related crimes are likely to engage multiple stakeholders in responding to their event(s) and mitigating future risks. IDCARE provides a central point to help clients develop tailored response plans to effectively respond to compromised personal information and systems. On average, clients engage IDCARE 2.1 times following an identity compromise and/or misuse event. Little is known about their journey post-IDCARE engagement.

This intervention aims to explore the journey of individuals who experience a particularly grievous identity compromise, namely an unauthorised mobile phone porting event. Such events are complex, compromising personal information to move a person's mobile phone number to another telecommunications carrier. Once criminal appropriation of identity information and then a mobile phone number occurs, further acts of identity misuse are possible. These subsequent misuse events can often result in money being withdrawn from an individual's bank account or unauthorised access to a person's email. Porting of a person's mobile phone account in order to intercept SMS-message verification codes is central to these acts. Once such codes are intercepted (because criminals now have control over the individual's mobile phone number), accounts with this form of second-factor verification are vulnerable.

As presented in Figure 2, this picture of the identity ecosystem is a complex one involving at least one form of identity credential compromise, an originating mobile phone provider, a ported mobile phone provider, and subsequent exploited entities following the interception of SMS-messaging (in this depiction it is the individual consumer's bank).

IDCARE anticipates these outcomes, if not already known by the client. The journey to prevent and respond is likely to be long, frustrating and generate mistrust of online and related communication technologies. This intervention seeks to understand this journey by interviewing previous IDCARE clients regarding their response pathways, their experiences and suggestions to improve practices across the Australian identity ecosystem.

Figure 2 Unauthorised mobile porting event

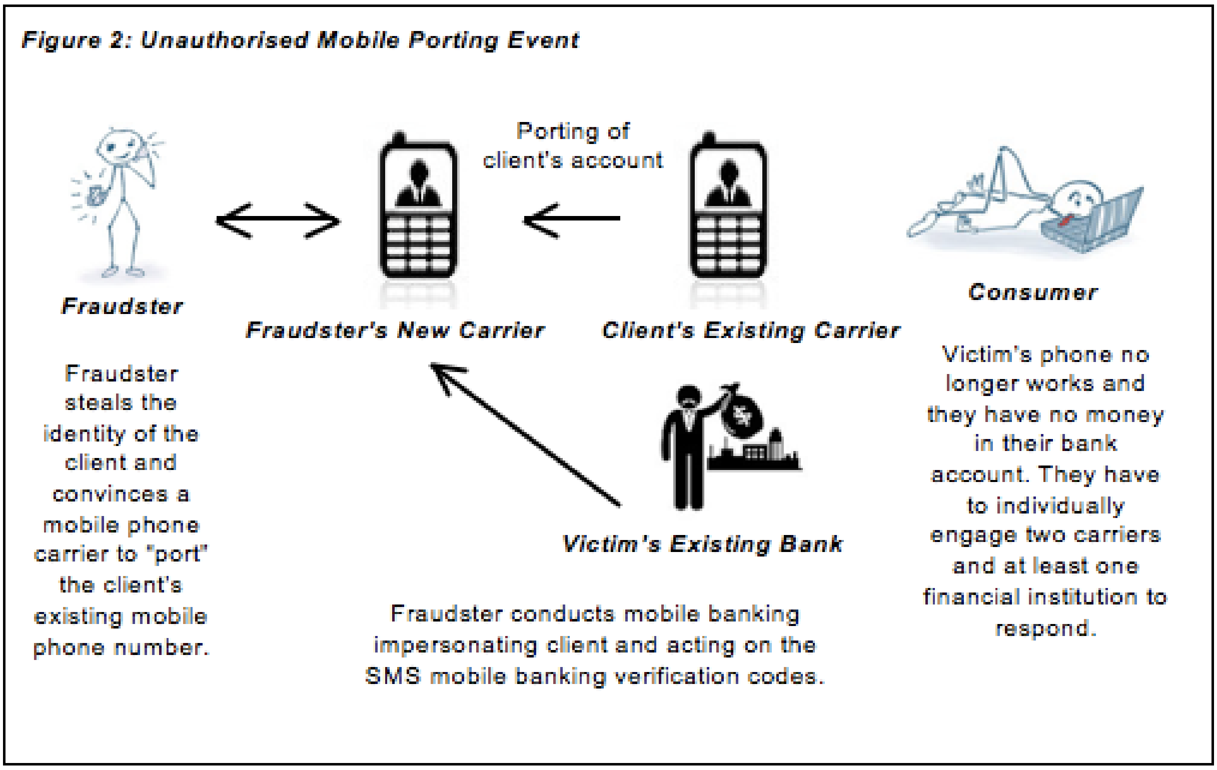


Figure 2: Unauthorised Mobile Porting Event
Porting of client's account
Fraudster
Fraudster's New Carrier
Client's Existing Carrier
Consumer
Fraudster steals the identity of the client and convinces a mobile phone carrier to "port" the client's existing mobile phone number.
Victim's Existing Bank
Fraudster conducts mobile banking impersonating client and acting on the SMS mobile banking verification codes.
Victim's phone no longer works and they have no money in their bank account. They have to individually engage two carriers and at least one financial institution to respond.

Approach

IDCARE engaged 131 former clients who had experienced the exploitation of their identity involving an unauthorised porting of their mobile service (inter-carrier port). There were 101 useable responses where the client consented to sharing their results anonymously for research, prevention and awareness raising activities.

Clients were selected based on their experience of an unauthorised porting of their mobile phone service between 1 September 2016 to 31 December 2016. This period was chosen to allow consumers sufficient time to respond following engagement with IDCARE.

The other stipulation for participation was that IDCARE had previously received permission from these clients to re-engage for research purposes. Of the 321 clients who experienced unauthorised mobile phone porting during the specified time, IDCARE received permission from 31.4 per cent for re-engagement. Follow-up interviews were conducted throughout March and April 2017.

A total of fourteen questions were asked of IDCARE's clients on re-engagement as part of a semi-structured interview (see Appendix). The questions asked were completed in full by 84 per cent of clients (85 clients), with only a minor number of questions not answered by the remaining 16 clients (identified in the Results and analysis section, below). The questions asked were categorised in relation to:

1. Identity ecosystem engagement experience and performance: examining whether clients of IDCARE completed the response plans advice provided, the time spent responding, and the satisfaction level attributed to response organisations.

2. Resolution and blame attribution: exploring the client's views around future identity compromise and/or misuse risks, whether the client's experience had been resolved (and what this actually meant), whether the client's views about IDCARE had changed since they last engaged the organisation, and whether the attribution of blame for their event had changed.

3. Direct impacts: examining whether the client had experienced any subsequent compromise and/or misuse, any psychosomatic impacts from the event (including behavioural change) and any other points the client wished to raise about their experience.

Results and analysis

The ecosystem engagement responses highlighted the variability in response standards. Approximately 83 per cent of clients who engaged IDCARE in response to their unauthorised mobile phone porting indicated that they followed the response plan guidance provided by IDCARE's Identity & Cyber Security Counsellors. On average, clients engaged 8.3 different business and government entities a total of 18.1 times after engaging IDCARE. It was estimated this took an average 11.2 hours of their time. Considering the average 8.3 hours clients had spent responding to their incident *before* coming to IDCARE (taken from a sample of 62 previous cases), it is not surprising that individuals considered the response time and complexity to have had the greatest impact on them throughout the experience.

Table 2 reveals the satisfaction scores of individual clients when reflecting on specific industry and government bodies. Each client was asked to provide a score out of ten on their overall satisfaction when engaging an organisation. The data was collected from all 101 clients interviewed and highlights the dissatisfaction towards ICT firms (including telecommunications carriers and resellers), law enforcement agencies, and credit reporting agencies. In probing this dissatisfaction, the overarching theme was the 'lack of empathy' and a 'failure to understand the broader identity risks to the consumer'.

Table 2 Client response satisfaction score by market segment

	Number of clients	Average satisfaction (*x*/10)	% of cases resolved
ICT providers	101	1.8	41%
Law enforcement	79	1.2	11%
Financial institutions	101	5.4	89%
Credit report agencies	84	1.5	72%
Utilities	21	4.3	93%
Commonwealth Government	64	5.5	91%
State / Territory Government	89	3.2	21%
Other	13	5.4	72%

Client satisfaction scores improved when telecommunications carriers, ISPs, and email services (such as Google, Apple and Yahoo) as well as law enforcement resolved cases, when compared with other engaged industries and sectors. Over half of all clients did not believe that ICT companies had satisfactorily resolved their matter. The most common complaint was the passing of clients from one telecommunications carrier to another to determine which personal information was used to initiate the unauthorised porting event. Two themes emerged from the qualitative information provided by clients in relation to this specific aspect. The first relates to mobile phone carriers and re-sellers not having requisite knowledge or systems that enable the easy retrieval of this information. This is particularly evident where one carrier believes the porting event landed with another carrier when, in fact, the porting actually occurred with the carrier's re-seller. This occurred in approximately 69 per cent of all unresolved cases.

The second aspect relates to what clients reflected upon as being a 'belief by the telco, that providing information about the porting event would breach the privacy of the criminal'. This occurred in almost a third of cases within the sample group that did not believe that their engagement with ICT providers was resolved (31 per cent, *n* 18 respondents).

'Resolution' had varied interpretations amongst respondents. To a large extent this was contextual. For example, 24 per cent of clients considered their position 'unresolved' when their state government failed to offer a different driver's licence number after their licence had been misused to initiate the unauthorised port. In other words, the risk of misuse involving the client's driver's licence endures for that individual.

In Australia, there are four credit reporting agencies and each offers slightly different practices despite consistent regulatory obligations. The Office of the Australian Information Commissioner requires a minimum 21 days ban on a credit file when requested by a consumer.

One of the four credit reporting agencies interprets this provision to mean 21 days as a *minimum* and asks individuals to nominate a period for the ban (in some cases individuals were offered six months). However, the three other agencies do not offer this flexible approach. They instead interpret the 21 days as a set period, with any period beyond this requiring an application for extension. The former agency also offers the individual access to their credit report, whereas the other three will only provide this if there is a separate application.

Clients viewed these inconsistencies as being the major irritant and dominant influence on their client satisfaction score. Other reasons for scoring that industry low compared with other engagement sites across the ecosystem related to having to apply online (especially when individuals had experienced an online withdrawal of their savings balance – i.e. a cyber crime) and generally being resistant to the reality that Australians have multiple credit reports from different credit reporting agencies and understanding the need for multiple engagements.

A total of 89 clients indicated a 'resolution' which appeared specific to the organisation they engaged and the outcome they required. However, a smaller number of clients considered 'resolution' in terms of whether they had experienced any further misuse from the initial compromise (12 per cent of clients interviewed). This was best described by one client as 'see no evil, hear no evil, therefore everything must be alright'. Despite only 11 per cent connecting 'resolution' with whether they had experienced subsequent misuse, the 'see no evil, hear no evil' response (or related response with the same meaning) was the most prominent captured across all clients.

'Resolution' was influenced by the specific requirements of each ecosystem organisation that was engaged. For example, the diversity of resolution included:

- Clearing any outstanding debt
- Informing the individual impacted precisely which of their personal information was misused in facilitating the unauthorised port
- Being reimbursed by the financial institution for the money that was accessed and transferred out of the individual's account
- Awaiting confirmation that their credit ban extension had been granted
- Awaiting confirmation by law enforcement that they would obtain a police report number
- Awaiting contact from the individual's ACORN report
- Awaiting an investigative outcome from law enforcement
- Awaiting a response from an ombudsman or an appeals process
- Awaiting for a credit report correction.

IDCARE was viewed favourably by most clients, with a client satisfaction score of 8.7 out of 10. The feedback echoed consistent themes, namely relief that a place existed where the individual could receive specific guidance and support irrespective of which organisation needed to be engaged.

However not all clients completed their response plans. Approximately one in four, or 17 per cent, who did not complete the response plan indicated not doing so because they were still awaiting advice from organisations they engaged across the ecosystem (for example, whether an unauthorised mobile phone port is a cyber crime and therefore should be reported to ACORN and not the local police station). Almost three quarters of the remaining clients who did not complete all of the response plans indicated that they did not have the time, or that obtaining one credit report and implementing one credit ban was sufficient (despite the recommendation to engage all credit reporting agencies). Lack of time was confirmed as a key influence in having to arrange multiple bans and reports, and then subsequent applications to extend bans.

System improvements may result from examining whether IDCARE could help arrange credit bans and reports on behalf of impacted individuals, assist communication between stakeholders (as a means to prevent further misuse), and work with law enforcement to get a report and report number.

IDCARE can reveal that the response journey for consumers is a rich picture of complexity, variable guidance across the network, and an overriding view of ‘see no evil, hear no evil’. A total of 84 clients revealed that they followed the IDCARE response plan. The balance of clients who did not mostly cited their inability to engage with specific actors due to the pathways these actors required them to pursue and their concerns about the exposure to re-victimisation (e.g. online provision of evidence of identity documents following a cyber-enabled misuse).

The preliminary findings indicate that most clients were dissatisfied with law enforcement (in particular ACORN) and the confused state between telecommunications carriers in correcting the unauthorised port and their financial institutions and law enforcement in providing critical information about what information was used by the criminals. The data collection has provided an opportunity to present anonymised case studies that highlight the complexity and at times dysfunctional response journey for consumers.

Perceptions of future misuse were high among participants, averaging 4.8 (or ‘High’). Clients who experienced an unauthorised port, the blocking of their email account, and withdrawal of funds from their savings account believed that future misuse was almost certain (average score of 5.8 out of 6, where 6 is ‘certain’ and 0 is ‘never’). This was particularly acute for individuals residing in states where driver’s licence numbers cannot be changed but it was the known source of compromise (*n* 23 clients averaging 5.3 or ‘Very High’ perception of repeat misuse). This contrasts with those who had only experienced the unauthorised porting and who knew that their passport was the compromise source (which they had cancelled). These participants were less likely to think that they would experience further identity misuse (average score of 1.3 out of six or 'very unlikely' to 'unlikely'). These results can be explained because a passport number does change when a new passport is reissued.

Blame attribution was captured in 81 per cent of clients (*n* 82). Of these clients, 54 attributed some blame in their initial reporting to IDCARE as captured between 1 October 2016 and 31 December 2016. Of these 54 clients, 87 per cent did not alter their perception of blame. The most common blame direction was the original telecommunications provider (62 per cent of the 54 clients where data was available to compare across both time periods). The second highest blame attribution event recorded, which remained consistent, was towards the telecommunications provider to which the mobile phone was ported (17 per cent of the 54 clients). The remaining clients blamed either themselves (9 per cent of the 54 clients) or their financial institution for allowing funds to be withdrawn.

What is interesting about blame attribution is the relative consistency in the direction of blame compared with when these clients initially engaged IDCARE. This implies that the response journey, with its own impacts on individuals, is unlikely to alter the individual's initial view of blame. The other interesting observation is a lack of awareness of how porting occurs (procedurally and technically) and whether those entities that are blamed could have prevented the unauthorised port. For example, individuals who blamed the original telecommunications provider are arguably blaming the organisation for 'losing' their business. The reality is that the entire telecommunications market relies upon churn and customer portability – arguably more so than any other industry. The consequence of this market setting is that a telecommunications provider can initiate a port without engaging directly with the originating provider. Advice received from the major Australian carriers indicates that this process is largely technical and automated in nature. It would seem that criminals are aware of this but consumers less so, hence the attribution of blame towards the originating telecommunications provider which may not even know the porting request has been made.

Blame towards financial institutions was only evident where the funds withdrawn had yet to be refunded by the financial institution – approximately 8 per cent of individual cases (*n* 8).

The final area of analysis examined whether individuals had experienced changes in their behavioural and physiological reactions to their event. A Likert scale was used against a variety of psychosomatic indicators of change. Clients, for the most part, maintained consistent behavioural impacts and emotions (such as feeling hopeless, fearful and down). However the physiological reactions did reveal change. For example, 31 per cent of clients indicated that they had felt physically sick upon when they first reported their experiences to IDCARE (between 1 October 2016 and 31 December 2016). Of these, 98 per cent indicated that they had stopped feeling physically sick after a short period post-engagement with IDCARE.

Intervention responses

IDCARE has further adjusted client engagement and response actions resulting from the findings of these two interventions. For example, IDCARE not only collects telephone scammer details but has established a new process of connecting this intelligence with the relevant carrier, re-seller or VoIP provider's privacy and security areas. This allows them to respond more immediately to the number being exploited on their network or with their service. Early experience with this changed process indicates that much more work needs to be done with these organisations around educating response options and exploring alternative intervention actions to disconnect known telephone scam numbers. A working group has also formed with brands targeted by telephone scammers across government and Australian-based private sector companies to further develop telephone scam prevention, detection and response measures. An initial pooling of known scam numbers had occurred and analysis commenced on this data feed to explore the particular signatures, modes operandi and dependencies within each telephone scam type.

Two distinct methods and tactics have emerged from this work: first, those telephone scams that seek to harvest payment and identity information (including direct payment while scamming on the call) and secondly, scams that seek to facilitate remote access of an individual's device to harvest financial and identity information. The latter can be particularly impactful for individuals as, recently, telephone scam that lead to remote access of devices have been detected as installing ransomware while in control of the device. This has resulted in a small, but increasing number of IDCARE clients experiencing further misuse through the activation of ransomware a short time after regaining control of their device and the subsequent impact of hard-drive damage and/or files lost or ransom payment made.

Work has also commenced with all major banks and the three telecommunications carriers to provide consumers with early warning that their mobile phone is about to be ported. Since December 2016, the three carriers have now implemented initial early alerting measures across a sample of consumers to examine business process impacts and formal adoption requirements as a business as usual process. These are encouraging signs and it is anticipated will lead to a reduction in subsequent misuse activity due to a more rapid response by consumers in protecting their accounts. Despite this, it is unlikely to result in a reduction in unauthorised porting.

Longer-term measures such as allowing consumers to change their driver's licence number are planned. The IDCARE Board is energised about this topic and has communicated key findings at the Australian Cyber Security Conference in March 2017 and the Privacy Awareness Week breakfast briefings in May 2017 across Australia and New Zealand. There is a need for stakeholders to recognise that the journey of their customers and clients is often as impactful as the initial compromise and misuse events. The time taken to respond, the number of engagements required, the dislocation and disparity of organisational responses, and the influences these have on blame attribution and perceptions of resolution are all important findings. IDCARE will brief the Board at its July 2017 meeting on these results which will, in turn, generate discussion on how the National Identity & Cyber Security Service for the Australian and New Zealand communities can build capabilities, influence change and drive consumer-driven solutions for those confronting these threats across the community.

Conclusions

This report aims to present an overview of the research team's intervention actions in communications-enabled identity theft events. The design of these interventions followed a detailed analysis of a sample of 4,000 IDCARE cases. Intervention in this context involved the adaptation of practice by IDCARE to better understand the complexity of communications-enabled identity theft, and inform individual and collective response efforts.

The first intervention activities resulted in IDCARE adjusting its data collection and processing activities to better understand what domestic infrastructure transnational organised crime is exploiting to enable telephone scams. Such scams were identified as being the number one contributor of identity theft compromise events in Australia that were reported to IDCARE and analysed during the preceding analytical phase of the research program. By capturing from IDCARE clients the precise number that scammers are calling from, this report was able to present key insights on organised crime's reliance on specific providers of domestic communications services. While a relatively small sample size, the results of this intervention highlight that a large portion of scam numbers are allocated and provided by exclusive VoIP providers. Further analysis revealed that the specific brands used by scammers and their modus operandi may also influence their choice of providers. For example, when scammers impersonate government, the results indicate that they are more likely to do so using major communication carriers than their re-sellers or exclusive VoIP providers. The results also indicate that the main brand targets of telephone scams are ICT providers themselves (such as Microsoft and Telstra). The report highlighted the distinctive method used in these scams when compared with scams that either seek to impersonate government, utility companies, financial institutions or fictitious entities.

This intervention has resulted in IDCARE adjusting internal processes and acting faster to reduce the time that scammers' telephone numbers are active on networks. This outcome will improve consumers' security and reduce risks around future compromise events. In addition, IDCARE has continued this work with its law enforcement partners in examining specific telephone scam signatures and related attributes to identify transnational crime groups.

The second intervention focused on response experiences of clients and complexity in the context of unauthorised mobile phone porting. This enabled IDCARE to re-engage clients and examine how its advice affected the resolution experience of its clients. The results provided important indicators that had been unrecognised in previous research. For example, the sample group highlighted the short-term nature of the physiological impacts from the initial identity misuse discovery (the mobile phone port and any subsequent misuse). Feelings and attitudes towards what 'resolution' looks like was a revelation. Resolution for a victim of identity theft does not readily equate to other crime types, particularly given that once an identity is compromised, it is compromised for life. In part, clients' resolution was contextual, directly related to an individual actor within the ecosystem. Great frustration was highlighted and directed towards communications providers for not efficiently communicating precise details of the unauthorised porting circumstance, including the identity credentials that were misused.

High levels of dissatisfaction were also recorded for law enforcement, and specifically ACORN, as well as credit reporting agencies. The reasons differed among responding groups. For example, the failure of law enforcement to meet a basic expectation that it would respond when a consumer complaint was lodged was a major feature of dissatisfaction. Dissatisfaction towards credit reporting agencies tended to be influenced by the time taken to receive support, the variability in customer processing requirements, and the number of engagements needed for consumers to secure a credit report and credit ban.

Blame attribution also presented interesting outcomes. Consumers appeared to not understand the process and technical constraints that exist in a highly competitive market where customer churn is an essential feature. The originating communication provider from which the phone was ported was seen by many consumers as the entity to blame for the unauthorised port. This is despite it not necessarily being able to initiate the port, nor stop its technical transfer quickly.

The insights obtained were not all negative for consumers. Commonwealth government, financial institutions and utility companies were seen more favourably in terms of responsiveness, and the view of IDCARE remained very positive. The outcomes of this intervention included many strategic initiatives across key market stakeholders to more rapidly transfer information and intelligence to and from consumers about the risks of unauthorised mobile phone porting. For example, the three major telecommunications carriers have agreed to communicate to consumers before an imminent porting event occurs and that contact should be made if the carriers had not initiated it. More work needs to be done to refine this new industry-wide control but it nonetheless represents a great opportunity to enhance the knowledge networks across the identity ecosystem, and in doing so, improve its overall resilience to identity misuse.

This body of work represents initial steps in gaining a much more detailed understanding of the ways in which Australia’s communications market is exploited by transnational crime and the impacts such threats pose to consumers both during and in the aftermath of these events. The interventions highlight the interdependencies across Australia’s identity ecosystem. The findings and outcomes emphasise the need for organisations to adopt consumer-centric approaches to identity theft prevention and response.

Appendix

<u>Intervention 2: Questions</u>

Identity Ecosystem Engagement Experience and Performance

1. Did you complete the response plan advice provided by IDCARE following your engagement? (Y/N/Still Completing)
2. What elements have you not completed? (ACORN, FI, Telco, CRAs, DL, ATO, AV, other)
3. How much time have you spent actioning IDCARE's response plan? (hrs est.)
4. Following your initial engagement with IDCARE what organisations did you engage? Industry/Service Type (Org 1, 2, 3)
5. Rate your satisfaction in engaging with each organisation? (score out of ten; ten being the highest satisfaction score)
6. What comments would you offer to Org 1, 2, 3?

Resolution and Blame Attribution

7. Has your experience been resolved? (Y/N/Unsure)
8. Rate the likelihood that you will experience further misuse of your identity? (Certain, Highly Likely, Likely, Unsure, Unlikely, Very Unlikely, Never)
9. Have you views about the support and advice provided by IDCARE changed? Explain.
10. Has your views about where you attribute blame for your experiences changed since engaging IDCARE? If so, in what way?

Subsequent Direct Impacts

11. Following engagement with IDCARE did you experience any further identity information 'compromise' or 'misuse'? If yes, what was this?
12. In what way, if any, has your behaviour changed since this event (Brief Symptom Inventory)?

Clients are asked whether they have experienced the following effects within a week of them knowing about the compromise/misuse of their identity information (5 point Likert-like scale response 0 = not at all through to 4 = extremely):

Somatization – Feeling weak, Nausea, Numbness, Faintness, Trouble getting breath, pains in chest;

Depression – feeling blue, feeling no interest in things, feeling lonely, feeling hopeless about future, feeling of worthlessness, suicidal thoughts;

Anxiety – feeling tense, nervousness, feeling fearful, spells of panic, suddenly scared, feeling restless.

13. Has there been any specific event, other than the compromise/misuse of your identity information that may have influenced this change in behaviour?
14. Are there other comments/views about your experiences?

Authors

David Lacey is Managing Director of IDCARE, Australia and New Zealand's National Identity and Cyber Support Service, and Professor of Cyber Security with the Centre for Human Factors & Sociotechnical Systems, University of the Sunshine Coast. IDCARE is a joint public-private sector innovation that provides a free helpline to the Australian and New Zealand communities who confront identity and cyber-related crime. As Managing Director of IDCARE, Dave works intensively across the community in advocating for identity and cyber security resilience and participant confidence. His teaching and research engagement with business and government leaders focuses on building consumer-centric approaches to cyber crime prevention and response.

Identity theft and Australian telecommunications:

Understanding the risks for consumers