AUSTRALIAN COMPETITION
& CONSUMER COMMISSION

# ACCC Submission to the Review of national arrangements for the protection and management of identity information.

November 2018

# 1. Introduction

The ACCC welcomes the opportunity to make a submission to the Review of national arrangements for the protection and management of identity information. The ACCC supports the view that the protection of identity information should be a key concern for the government and the community given that identity crime is one of the most common crimes in Australia costing over $2.2 billion every year.[1]

As you may be aware the ACCC is an independent Commonwealth statutory authority whose role is to enforce the *Competition and Consumer Act 2010* (the Act) as well as a range of additional legislation, promoting competition, fair trading and regulating national infrastructure for the benefit of all Australians. The Australian Consumer Law (ACL) is contained in Schedule 2 of the Act which sets out Australia's consumer protection regime.

The ACCC manages the Scamwatch website (www.scamwatch.gov.au) which gives information to the public to help them recognise and avoid common scams and provides an online service for reporting scams. So far in 2018, this service has received over 132 000 scam reports with 8.5 per cent of these reporting a financial loss. The total financial loss reported so far in 2018 is $94.3m. This submission provides an analysis of reports to Scamwatch, an explanation of the ACCC's role in relation to scams and recommendations for consideration which may bolster the protection of identity information in Australia.

Australian businesses and consumers regularly engage in online trade and commerce and their everyday communications are now more than ever conducted over a range of social media platforms, telecommunications and online services. The use of these services and the availability of personal information creates opportunities for cyber criminals to cause widespread detriment to Australians through identify theft and related crime.

The ACCC is currently undertaking an inquiry into digital platforms which will consider issues relating to information asymmetry between digital platforms and consumers. The Inquiry may result in a range of outcomes including recommendations to Government. A Preliminary Report is due to be provided to the Treasurer by 3 December 2018. We intend to provide a copy of this report, once published, for consideration by the Review.

Many businesses who offer "free" services to consumers do so on the basis that they are collecting significant amounts of personal data in exchange for the "free" service. The business model of digital platform operators is premised on the collection of large amounts of personal information. This has also dramatically increased the volume and granularity of personal information available. Consumers are often unaware about how much of their personal information is collected by digital platform operators, how they use it or who else has access to it. This restricts their ability to make choices and also potentially has long term consequences (for example identity theft, hacking).

While advances in technology and new markets have led to greater efficiency and choice for Australian consumers and businesses, it has also highlighted emerging risks for individuals, businesses, regulators and the broader economy. The sheer volume of personal information and data that is obtained, stored or transacted every day increases the vulnerability of consumers and businesses to inadvertent misuse or deliberate theft of their personal information which can lead to financial detriment and other harms.

The ACCC is not responsible for the regulation or enforcement of privacy laws. However, failures by private organisations and government to protect personal information will inevitably reduce trust and confidence in markets. Consumers and businesses want to

[1] Attorney-General's Department, *Identity crime and misuse in Australia 2016*.

ensure that their information is protected from data breaches, identity theft, online fraud and scams.

# 2. Scamwatch reports

The ACCC reports annually on the impact of scams in Australia.[2] For the purposes of this submission, scam is defined broadly to include fraudulent or dishonest activity by individuals, groups or businesses to attempt to gain money or information, either through direct misrepresentations to a victim, or indirectly (often without their knowledge) for example by stealing documents or accessing accounts. In 2017, Scamwatch received over 160 000 scam reports with $90.9m in financial loss. Combined losses including reports to the Australian Cybercrime Online Reporting Network (ACORN) were $340 million. The ACCC notes that the losses for scams reported to the ACCC are just a small portion of the real impact on the Australian community.

The Scamwatch report form allows consumers to report the category of scam and the loss including financial and/or the loss of personal information. Reports to Scamwatch indicate that many scammers are seeking to obtain personal information so that it can be used to access a person's finances directly or indirectly through access to other services. Our data highlights several areas of concern for Australian consumers in relation to the loss and misuse of identity information.

**Attempts to gain personal information**

Scamwatch collects a range of information about scams, the reporter and the scammer. When a consumer lodges a report they are prompted to choose a category of scam, one of which is *attempt to gain your personal information*. There are four sub-categories which include: phishing; identity theft; hacking and remote access scams.

As at 31 October 2018, Scamwatch received 45 884 scam reports in the category attempt to gain your personal information, and 4 per cent of these also reported financial loss which totalled $8 463 562. Most financial loss occurred where the victim was contacted over the phone ($4.8m) or email ($2m). Those aged over 65 made the most reports (8 692) and lost the most money ($2.9m). Reports and losses for this category have increased when compared to 2017. We note that losses reported to Scamwatch remain a tiny percentage of the losses to identity theft and that the full extent of losses is usually not known until long after the identity theft occurs.

*Hacking*

In terms of the subcategories, there were 6 944 reports about hacking with over $2.2m in financial loss. Most were contacted via email and the most money was lost by people aged 35-44 years old.

*Identity theft*

There were 10 195 reports about identity theft with $1.3m reported lost. Reporters were most commonly contacted over the phone and the age group that lost the most money was 25-34 year olds. The ACCC notes that many consumers report identity theft to other organisations such as ACORN. In 2017, reports to ACORN included $43m in financial loss to online identity theft.

*Phishing scams*

[2] https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

There were 19 169 reports about phishing with $579k reported lost. The most money was lost by those over 65. In 2018 more money is being lost to phishing scams over email when compared to 2017 when it was more commonly lost over the phone.

*Remote access scams*

Remote access scams have caused more harm to Australians in 2018 when compared to 2017, particularly to older Australians. Scamwatch has received 9 567 reports so far in 2018 with 8.2% reporting financial loss totalling $4.4m. Losses to these scams have almost doubled when compared to 2017 ($2.4m lost). In 2018 over $2m has been lost by people over 65 years old which is three times what was lost by this group in 2017.

**Loss of personal information**

The Scamwatch report form also allows consumers to report what type of loss they suffered for any of the scam categories. Many consumers report losing personal information, money or both. The number of reports to Scamwatch about the loss of personal information appears to be increasing.

In 2017, 21 424 (13.26%) of the 161 528 reports made to Scamwatch (across all categories) indicated the reporter suffered a loss of personal information, with total losses of $11 805 527 across these reports.

By comparison, the data for 2018 (up to 31 October 2018) shows that in 21 615 (16.13%) of the 132 617 reports, the reporter indicated a loss of personal information, with total losses of $20 374 678 across these reports.

This increase may indicate that more scammers are targeting personal information or that Australians are more aware of the loss of their personal information. In terms of age, there is no particular age group that reports the loss of personal information significantly more than others, except that those under 24 report the least.

We analysed the reports where loss of personal information was recorded in terms of the category of scam and age of reporter as outlined in table 1 below.

**Table 1 - Percentage of reports indicating actual 'Loss of personal information' by age group and scam category in 2018**

| Age Category | Top 3 Scams | Number of reports | Percentage of reports for age category |
|---|---|---|---|
| Under 18 | Online shopping scams | 29 | 16.29% |
| | Phishing | 22 | 12.36% |
| | Hacking | 19 | 10.67% |
| 18-24 | Identity theft | 214 | 13.18% |
| | Jobs & employment scams | 185 | 11.39% |
| | Online shopping scams | 155 | 9.54% |
| 25-34 | Identity theft | 559 | 17.07% |
| | Online shopping scams | 295 | 9.01% |
| | Phishing | 259 | 7.91% |
| 35-44 | Identity theft | 481 | 16.43% |
| | Phishing | 222 | 7.58% |
| | Online shopping scams | 196 | 6.70% |

| | | | |
|---|---|---|---|
| 45-54 | Identity theft | 346 | 13.49% |
| | Hacking | 243 | 9.47% |
| | Dating & romance scams | 221 | 8.23% |
| 55-64 | Identity theft | 373 | 15.87% |
| | Hacking | 275 | 11.70% |
| | Remote access scams | 214 | 9.10% |
| 65 and Over | Remote access scams | 477 | 15.99% |
| | Identity theft | 455 | 15.25% |
| | Hacking | 355 | 11.90% |

In addition to hacking, identity theft, phishing and remote access scams, consumers (particularly in younger age groups) are also losing personal information to online shopping scams; jobs and employment scams and dating and romance scams.

The top two contact methods for scams resulting in the loss of personal information in 2018 were 'Phone', with 7958 reports (36.82% of all 2018 reports to 31 October resulting in the loss of personal information) and 'Email', with 6158 reports (28.49% of all 2018 reports to 31 October resulting in the loss of personal information).

**Misuse of personal information**

For most consumers it will not be clear how their personal information was used. More consumers report experiencing a 'loss' of personal information than explain specifically how it was misused. Scamwatch reports highlight the following common uses of identity information obtained by scammers:

- Accessing the victim's bank account/s and transferring funds out
- Charging goods and services (utilities, Uber, take-away, etc.) to the victim and taking out lines of credit, or phone plans in the victim's name.
- Creating new bank accounts in the victim's name and using victim bank accounts for money laundering.

Scammers often use the personal information obtained to escalate their access to the victim's identity before being able to steal money by:

1) Porting the victim's phone to a new number under the scammer's control in order to bypass two factor authentication.
2) Using personal information to access the victim's social media to gather more personal information
3) Using personal information to access the victim's email to gather additional personal information, receive password reset emails and bypass two factor authentication.

Other uses for illegally obtained identity information may include being placed onto contact lists passed between scammers resulting in unwanted contact via phone calls, SMSs, or emails.

# 3. Case Studies

The following case studies are reports to Scamwatch from the public which illustrate the most common fraudulent uses for identity information. The reports are modified to protect the privacy of the reporters.[3]

1) **Report of phone porting to bypass two factor authentication**:

A thief used my Medicare card for the ID required to set up a prepaid phone service with Vodafone without my authorisation. My phone number was then ported from Aldi Mobile to Vodafone.

The thief then used the two step verification feature on Facebook and PayPal to reset a "forgotten" password, create a new password and access those accounts. I received an email notification that those passwords were changed and quickly took control of those accounts by changing the password and removing the mobile number from Facebook and PayPal. The IP address provided by Facebook for the thief was in Belmore Sydney, NSW.

Around two hours later someone accessed my email address and removed my recovery email address from it. Google account history shows this person was located in Gostivar, Macedonia. I changed all email passwords, removed the compromised phone number and enabled two factor authentication via the Google Authenticator phone app.

Since then someone has set up an email account using my best friend's name and sent me a targeted phishing email.

2) **Report of substantial monetary loss as consequence of personal information loss**

At approximately 2.30pm my iPhone's network coverage ceased suddenly with my provider Optus. I contacted Optus who advised that they had a record that I had updated to a new sim card that day - which I had not. However they did not flag an issue with this. They recommended I go into an Optus store to obtain a new Sim card.

I went to the Optus store about 5pm to get a new Sim card. I activated the new Sim card about 9.45pm. This worked and I again had access to my Optus network.

About 11.25pm I logged onto my ANZ bank account - it had a credit card, cheque and home loan accounts linked. It was evident that there had been **$88,600** withdrawn from the cheque account. I immediately contacted ANZ in regards to this.

I have since identified that ANZ sent two replacement credits cards to myself and my partner in the weeks before this incident. We never received these credits cards so believe that they were stolen as they were in transit to us or from our letter box. Someone has gained access to my mobile by activating a new Sim on a new phone. I can confirm that they accessed my Gmail account on an Iphone 6S. I received a call from a private number around this time from someone claiming to be ANZ customer service. They stated that I needed a new credit card and that they would send this card to me. They read out my address to me and asked me to verify it over the phone which I did.

3) **Report about identity verification by telecommunications provider**

I am with Optus and received a message from Vodafone saying that my number has been successfully ported. I had never contacted Vodafone or Optus to change providers. My phone went straight into SOS mode and I then started getting Netbank

[3] Reports are reproduced largely as reported by the consumer, however small edits are made to improve readability, fix errors, remove personal information or reduce content.

notifications that my withdrawal limit has been changed. I was at home with Wifi so jumped on to my laptop and saw that money **($18 750**) was transferred out of my account. I'm a single mum with three kids and no access to another phone so I had to visit a police station at 8pm at night with three kids in tow to call the bank to freeze my account.

I went into the Optus Store the next morning and they said I no longer had an account with them and that someone went on to Optus Online Chat earlier asking for my account information and all Optus asked for was for my name, date of birth and address and then gave away my personal information to this person in which they then ported my number. Since then it's been a week and I still don't have my number back and I've been through hell and back with Optus. So furious that it can take 2 seconds for someone without showing ID to illegally port my number but for me to get it back I've been back and forth with Optus, they've had to sight ID numerous times and it's still not up and running.

4) **Report of credit card mail fraud**

We changed banks and were expecting the credit card in the mail which took longer than expected but the bank wouldn't let us pick it up from a branch.

On the 13/10/17, a man called me from a "blocked number" pretending to be from immigration asking security questions in regards to my Visa. I clarified that I am a resident and that they can send me any information via email. He was very pushy but had my husband's e-mail and my passport number and made me confirm the details and used my voice to activate my new credit cards. Three days later my phone lost signal, I was at work and called Vodafone in the evening.

During that time they activated the cards and used them in Coles, Harvey Norman and a petrol station. They stole my number and were answering my calls on a mobile on their end approving all payments until we noticed and applied a ban on my number. They kept using the cards and when the bank couldn't reach my number, they rang my husband to approve the payment and that's when we proved everything by checking the transactions with the bank. They took **$3000**.

We filed a police report on the same night and it took them 8 weeks to get back to us. Despite me trying to follow up, the police made it clear that they had more important matters involving life threatening situations. Since my identity was stolen they were able to steal our new cards from the mail again six weeks later when we ordered cards from a different bank. The police never did anything about it and the criminals are still free.

5) **Report of multiple misuses of stolen personal identification information**

A scammer has opened 6 fraudulent bank accounts, a loan, credit card, a mobile phone plan with Telstra and gained access to my Medicare card. Accounts with Latitude Finance Australia; Credit Corp Financial Services Pty Limited; Commonwealth Bank of Australia, 3 Accounts with National Australia Bank; A loan and credit card with ANZ.

I received a Certificate for a victim of Commonwealth Identity Crime, but it did not help me to change my driver's licence number which I need to do. The WA law doesn't allow me to. I feel I could protect my identity if I can change my driver's licence number.

6) **Report of remote access scam**

I was called on a landline by a man who said he was from Telstra fraud department and that there had been a firewall failure and fraud was contacting customers to help with online fraud. They had me download *Teamviewer* so they could access my

computer and cell phone. I was asked to check my bank accounts and was assured they couldn't see my password. I did this quickly and closed the accounts on both CBA and Westpac.

I didn't realise this was a scam as I've lived in the US and returned only 9 months ago. I was unaware I had been scammed until friends told me 5 days later. I went to the police and realised that my Westpac account had been blocked but my CBA online banking was still open. From my CBA account only they transferred most funds between 2am and 3am. I turned off my computer after calling CBA to close my online banking on Sat 30 June. I had my computer IOS system reinstalled on Monday. CBA Bowral on Monday told me I hadn't lost any funds but I learned on Tuesday with my personal banker that considerable funds had been lost (**$125,000**).

The CBA fraud department was contacted immediately. The scammers transferred to a new payee about $19,600 each day and an additional $26,400 on the last day. Once I had access to my online banking again I learned that the scammer was a CBA customer! CBA couldn't recover my funds.

# 4. Enforcement

Scams are essentially crimes of deception. Some scams if tested in court may be breaches of the Australian Consumer Law (ACL). However due to the 'fly by night' nature of many scammers, it is difficult for law enforcement agencies to track them down and take action against them. This is further complicated by the fact that most scammers are based overseas. The perpetrators can be individuals, or organised criminals who set up schemes that are difficult to trace, based overseas and occur over multiple jurisdictions. Scammers take advantage of instant and anonymous communication channels to connect with targets, and are quick to morph and phoenix operations into a new scam when authorities close in.

The ACCC published its compliance and enforcement priorities annually. Currently in relation to scam conduct, the ACCC prioritises awareness raising and education and working with government and the private sector to reduce opportunities for scams to occur. We analyse data collected through our Scamwatch service to identify trends, monitor financial losses and inform our scam prevention strategies. On behalf of the Scams Awareness Network, the ACCC runs Scams Awareness Week, an annual campaign to warn consumers about the ongoing risk of scams. In addition, the ACCC is also working with the banks and other intermediaries to share information about scams and encourage them to take a more proactive approach to prevent their customers falling victim to scams.

Identity theft is a challenging activity to detect and enforce. Many people will fall victim to a data breach by a government agency or private organisation but will not generally be able to detect how there information was misused, including whether it fell into the hands of a scammer. Therefore careful protection of personal information should be a priority for business compliance and government.

# 5. Recommendations for consideration

Existing laws, awareness raising efforts and IT security systems are already in place to mitigate the risk of identification loss and subsequent misuse by criminals.

The following recommendations provided for consideration are aimed at further reducing identification information loss and misuse for consumers. As noted above, recommendations arising from the ACCC's Digital Platforms Inquiry may also be relevant to this Review and once published will be provided to the Review.

## 5.1. Create larger financial penalties to ensure organisations comply with secure storage of data

Data breaches of large organisations can potentially affect millions of people. Australian and international companies are at ongoing risk of data breach by cybercriminals and need to proactively protect and monitor the security of their data.

Consideration should be given to increasing the financial penalties for businesses which do not adequately secure customer data. This may incentivise businesses to implement and maintain better security and protection for consumer data.

## 5.2. Examine existing phone porting regulations

Mobile phones now contain a large amount of personal information and are regularly used for security verification for a range of utilities and accounts. Mobile number porting occurs when a mobile number is transferred from one telecommunications provider to another. This happens legitimately whenever a consumer changes their provider to seek a better deal. However, scammers can do this without the knowledge of the number's owner and set up their own mobile phone to receive messages to the ported number. This is usually done to intercept two-step authentication messages from banks or service providers.

Scammers will usually have already obtained access to some of your personal details including your data of birth, phone number and address via your social media profile or other information they have obtained about you. Once they have your mobile number they have access and control of your mobile service including calls and texts. Once ported the scammer uses your mobile account to gain access to email accounts and bank details. Any verification codes sent by the bank for large money transfers will then be sent to the scammer instead enabling them to steal money from you.

Phone porting requires relatively little personal information (e.g. name and date of birth) but establishes a foothold for criminals to gain access to other services, including access to bank accounts. For example, a provider advises on its website that "*You'll need to be the Rights of Use holder. You'll also need to provide the account number of the current service provider or your date of birth. This information is used to validate your details with your current service provider*." The ACCC recommends hardening the defence to this vulnerability.

Telecommunications companies and the Australian Communications and Media Authority (ACMA) should re-examine phone porting regulation and systems with a view to ensuring there is a more robust and secure process in place while maintaining competition between telecommunications providers. For example, telecommunications companies should be required to increase the identity information they require before porting a number, or they should consider confirming that a port has been requested before proceeding.

Similarly the banking industry which encourages consumers to use their mobile phones as a security measure (by sending transfer authorisation codes to mobile phones) should consider working closely with the telecommunications companies to address this vulnerability.

## 5.3. Provide better protection against personal information mail theft

While online loss of identity information represents the largest threat currently, theft of physical mail is another way in which identity can be stolen and misused. Apartment buildings with banks of mailboxes may be particularly vulnerable.

Agencies that send personal information by mail need to ensure these are being sent in a secure manner. Specifically, driver licenses, Medicare cards, senior's cards, bank (credit) cards, and even utility bills should not be sent through standard mail. These types of documents or cards can facilitate identity theft and can be either stolen from a mailbox or mail redirections can be set up by scammers to gain access. It is preferable that consumers have the option of receiving important identity documents or cards either by registered post or picking them up at a storefront or branch.

Consumers may be more exposed to mail theft as a result of changes to delivery schedules. Mail is now delivered to Australians every 2 or 3 days which means consumers are less likely to be checking and collecting their mail every day.

Utility bills should be provided electronically rather than physically where possible. Utilities should follow similar practices to the banks and notify a consumer that their bill is available in their online account (which requires them to login) rather than sending account information directly over email. Physical personal information cards as mentioned above should be sent by default as registered mail with consumers provided the opportunity to opt out.

The introduction of a voluntary code for document issuing organisations to adhere to security conscious practices when issuing and delivering identification documents may be a solution for establishing best practice.

## 5.4. Discourage identity verification by biographical information

The biographical information (that is, name, address and birthdate) of Australian consumers is provided to many unknown parties over the internet, and through loyalty programs. Online shopping requires the provision of an address for Australians without a post office box. Many websites offer incentives such as rewards points or discounts for registering an account with their basic details including date of birth and address.

The ACCC is concerned with the ongoing use of this relatively easily obtained information as a proof of identity in commercial contexts. Business that rely on biographical information for identity confirmation and security purposes are playing into the hands of fraudsters and scammers. The reliance on biographical information in proving identity should be reduced. We recommend encouraging the adoption of two-factor authentication in lieu of, or always in addition to, basic biographical information for proof of identity in commercial contexts.

The ACCC sees merit in pursuing the adoption of biometric verification in line with the National Identity Security (NIS) Strategy. For the present, it acknowledges some companies including small businesses are unable to implement identity checks using biometric information, and would be unable to store such information securely in line with the Privacy Act.

The ACCC notes that while businesses have benefited from reduced costs associated with the increasing digital environment, they should not spare expense in protecting identity information of their customers. In addition, where businesses use biographical information which leads to a consumer falling victim to identity theft, the business should be under an obligation to assist the consumer as much as possible to address any fraud that has occurred and minimise further compromise of their identity information.

## 5.5. Improve resourcing for victim care providers

Identifying and rectifying the range of practical impacts from a personal information breach is impossible for most Australian consumers. Direct communication with a victim to address the psychological effects of such losses is also crucial.

IDCARE's submission to the Attorney-General's Department Serious Data Breach Notification Consultation in 2015 stated,

> "Approximately one in five IDCARE clients present psychological and somatic symptoms and impacts following the compromise of their personal information."

In Australia and New Zealand, this gap has been filled by the IDCARE charity since 2014, prior to which there was no dedicated support organisation. IDCARE provides free education, awareness, and practical support in the form of one-on-one counselling and customised response plans to members of the community with concerns about their identity or related cyber security. In a 2016 interview, Managing Director David Lacey of IDCARE reported the organisation spent on average 19 hours with each individual client.

The major Australian government fraud and identity crime reporting portals –the Australian Taxation Office, Department of Human Services, Office of the eSafety Commissioner, the Australian Cybercrime Online Reporting Network and the ACCC's Scamwatch – all direct reporters of identity theft to IDCARE.

Despite receiving over 30,000 individual contacts since its inception in 2014, IDCARE operates on a modest annual budget. Its last report to the Australian Charities and Not-For-Profits Commission recorded its expenses at $199,308.00 for the 2016-2017 financial year, 48.12% of which was spent on its employees. The majority of IDCARE's staff are volunteers, sourced from partner universities.

The ACCC recommends consideration be given to:

- creating additional grants for individuals and organisations providing remediation, counselling and education services for victims of identity theft
- providing direct government funding for IDCARE, additional to its current funding model of grants, cost recovered services and member organisation subscriptions. Additional funding would allow for more staff and better support for victims of identity theft and related issues.

## 5.6. Support consumer education about personal information protection

Consumer education plays a crucial role in protecting Australians from personal information loss and misuse. The Australian population has gaps in digital literacy, information security fundamentals, and understanding of the value of personal information.

Many losses of personal information reported through Scamwatch were preventable with additional education. While it is important not to place blame on victims, all Australians would benefit from greater awareness about how they can protect their personal information and minimise the risk of falling victim to scams. Scammers hone their craft over decades and scams can be difficult to detect for even the savviest consumer.

We recommend consideration be given to increasing the focus and funding of consumer education for personal information protection across Australia particularly for those who may be disadvantaged and vulnerable.