
Veda 2015
Cybercrime
and Fraud
Report

Contents

- 02** Introduction
- 03** Cybercrime and fraud in 2015 – a snapshot
- 06** Cost of cybercrime and fraud
- 09** Where do the fraudsters come from?
- 10** Consumer attitudes to cybercrime and identity theft
- 13** Data breaches
- 15** Combatting cyber fraud
- 19** Looking ahead – cybercrime and fraud in 2016
- 20** For more information

Introduction

Veda is a data analytics company and the leading provider of credit information and analysis in Australia and New Zealand. Combining more than 47 years' experience with information on around 20 million credit-active individuals and 5.7 million commercial entities, we offer powerful systems, intelligence and analysis. We accumulate and transform data into meaningful insights, which enables both consumers and the diverse businesses we partner with to make proactive, responsible and informed decisions.

Veda operates within the fraud and online security sector with Australian businesses, governments, enforcement agencies and individuals, to provide shared insights, analysis and anti-fraud products and services. Our work gives Veda deep insights into cybercrime and fraud.

Some of our insights have been compiled into this annual **Cybercrime and Fraud Report**.

Cybercrime continues to evolve and morph as cyber criminals respond to security and technology improvements. Common types of cybercrime include identity theft, online scams, fraud involving the buying or selling of goods online (card not present) and hacking into online accounts. The commonality in cybercrime is the criminal's objective to steal information from victims for their own benefit.

Stealing personal information from individuals allows criminals to do more than just steal money. They may also create rumours, conduct illegal activities, perform blackmail or expose sensitive facts about individuals, firms or governments. They may use a victim's account as a mule account to launder money or finance terrorism.

The credit industry is a particularly high profile target for cyber-criminals because of the potential direct access to financial gain.

The mechanism to extract financial advantage depends on the sophistication of the criminal. Through phishing or a direct hack, a criminal may access a password and username that allows them to operate a victim's online account for the purposes of transferring funds or buying goods and services. A more sophisticated crime might involve the theft of a person's identity, so criminals can buy and sell assets or apply for credit in the victim's name.

This report provides insights into the frequency, types and trends of cybercrime and fraud in Australia in 2015. It canvasses consumer attitudes towards credit cyber fraud, and expectations for how credit providers should be responding. This report draws on exclusive data and insights from Veda's Shared Fraud Database, insights from government and industry agencies and insights from Veda consumer research.

It is a useful resource for any organisation or individual who is the target of cyber fraud or wants to know more about how to combat this growing threat.

“Financially motivated criminals that exploit and access systems for financial gain are a substantial threat to Australia. Transnational serious and organised cybercrime syndicates are of most concern, specifically those which develop, share, sell and use sophisticated tools and techniques to access networks and systems impacting Australia's interests”.¹

Australian Government's Australian
Cyber Security Centre 2015 Threat Report

Cybercrime and fraud in 2015 – a snapshot

Highlights:

1 in 4 Australians have been a victim of identity theft – 25% reported having been a victim (up 7% 2014/15 compared to 2013/14) (Source: Veda Consumer Survey)

12.6% Reported volume of online credit application fraud incidents by Veda Shared Fraud Database members up 12.6% 2014/15 compared to 2013/14

50% of credit application fraud in Australia now occurring online – an increase of 33% compared to the previous financial year. This compares with a 23% fall in credit application fraud incidents occurring at bank branches in 2014-15 compared to 2013-14 (Source: Veda Shared Fraud Database)

59% Fraudulent credit applications involving identity takeovers in Australia rose 59% in the past two years – and 17% in the past 12 months (Source: Veda Shared Fraud Database)

Insights from the Veda Shared Fraud Database show a tipping point in credit application fraud has been reached.

Fraudsters are now more likely to apply for credit online than fill in an application form in a bank branch. This is being driven by industry moving to online applications.

A second key trend is that as credit providers toughen up rules and technology for the verification of identity, providing a false identity has become less viable for fraudsters.

Instead, identity takeover, where the bona fide identity of an individual (or entity) is stolen and operated for the purpose of applying for credit, is becoming more attractive for criminals. This type of fraud has grown 59% in the past two years.

The opportunities for criminals to use real identities instead of fictitious identities is being fuelled by the number of data breaches seen in Australia with well-known dating, retail and government databases being compromised.

Figure One: Proportion of Fraud Sub-Types as a % of all confirmed fraudulent credit applications, Veda Shared Fraud Database 2014/2015.ⁱⁱ



% Share FY15	58%	22%	9%	8%
Fraud Sub-Type	Falsifying Personal Details	Identity Takeover	Undisclosed Debts	Fabricated Identity

Note: Products and fraud types with low volumes have been excluded

There are four main sub-types of credit application fraud:

- 1. Falsifying Personal Details** (such as falsifying payslips, bank statements and tax assessments)
- 2. Identity Takeover** (using someone else’s identity or identification documents, to apply for credit)
- 3. Undisclosed Debts** (omitting or deliberately lying about financial commitments)
- 4. Fabricated Identity** (creating a fake identity, most commonly through the fraudulent creation of a drivers licence, passport or bank statements)

Figure One shows the proportional occurrence of each of these four sub-types of credit application fraud in 2015.

While identity takeover is growing, **falsifying personal details** remains the most common attempted credit fraud.

According to Veda’s Shared Fraud Database in 2015, payslips were the most common document falsified, followed by bank statements and tax assessments. This suggests fraudsters are not surprisingly seeking to falsify income and their financial status to gain financial advantage.

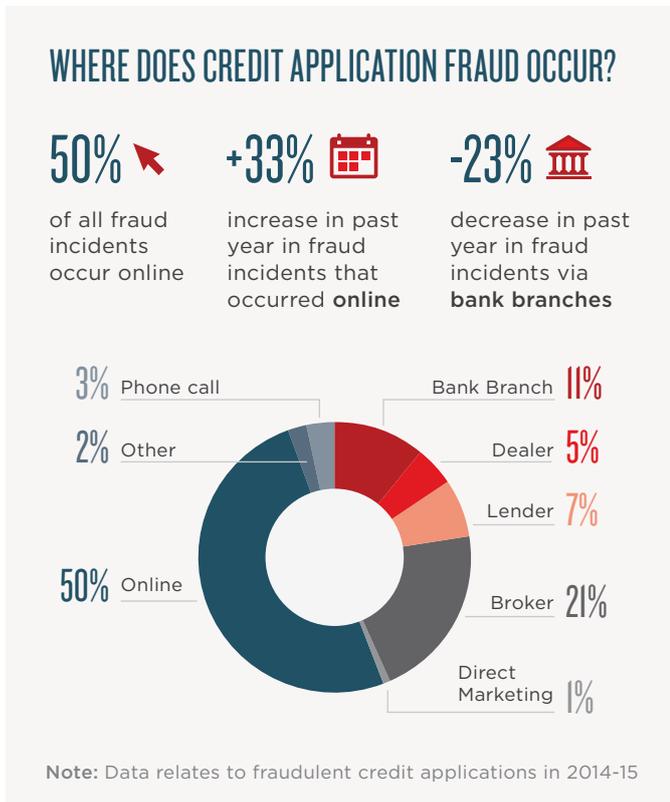
Drivers licences were the most common document put forward by fraudsters when they attempted the **takeover of an identity**. To meet application criteria, payslips, bank statements and utility bills in the name of an acquired identity were commonly used as part of identity takeover fraud.

Of the 126,305 fraud and deception offences recorded by police agencies in 2013/14, 40% (almost 50,000 cases) involved identity crime.ⁱⁱⁱ

While not all these offences would have involved credit fraud, these Australian Government statistics underline how prevalent identity crime, including identity theft, is in Australia.

Similarly to identity takeover cases, drivers licences were the most commonly used document to support a **fabricated identity**, and, fabricated passports were more common in this type of fraud.

Figure Two: Channel source of fraud as a % of all fraud, Veda Shared Fraud Database, 2014/2015.^{iv}



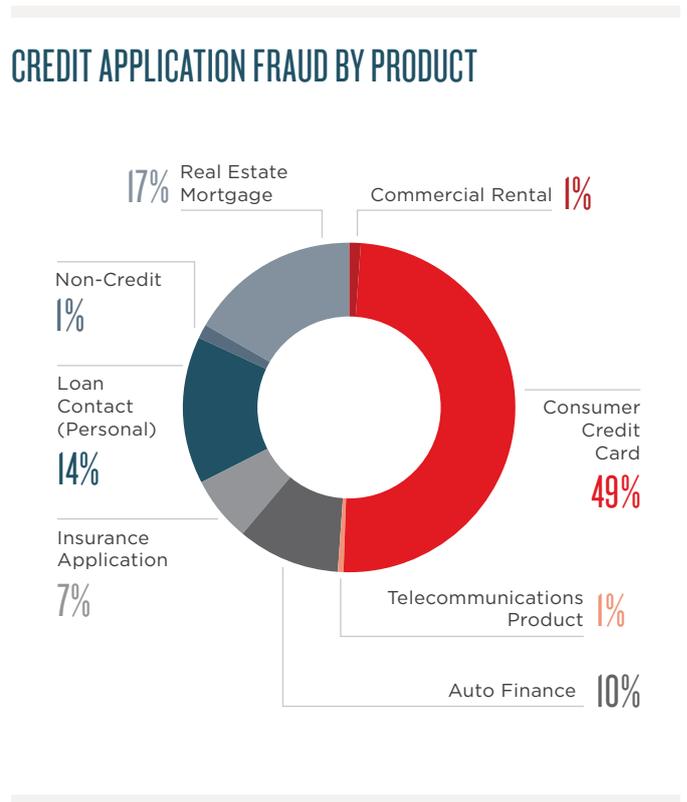
With the growth of the delivery of financial services online and other e-commerce, online credit **application fraud** is now the most common form of credit application fraud and has grown 33% in the 2014/15 financial year.

The broker channel is also of concern, with fraud occurring at broker increasing 24% from 2013/14 to 2014/15. **Broker fraud** now represents 21% of all credit application fraud.

Fraudulent credit applications in branches is falling (-23% in 2014/15) and now represents only 11% of credit fraud.

Consumer credit cards are the target of the majority of fraudulent credit applications, up 28% in 2014/15 and now representing 49% of all credit fraud. The most common fraudulent activity with cards was the presentation of false personal details, but it is important to note that cards had the highest proportion of fraud involving identity takeover (37%) of any

Figure Three: Product type % of total fraud Veda Shared Fraud Database 2014/15.^v



product category apart from telecommunications (telecommunications represents less than 1% of total fraud, so the high proportion of identity takeover is not significant in the wider picture of credit application fraud).

Fraudulent mortgage applications represented 17% of attempted fraud, down by 4% for the year 2014/15.

Personal loans represented 14% of fraudulent applications, up 7% in 2014/15.

Veda's Shared Fraud Database data is consistent with an Australian Institute of Criminology survey (2014), cited in the Australian Government's Identity Crime and Misuse in Australia 2013-14 Report^{vi}, which found consumers reported credit card information as the most commonly abused for identity theft or misuse, followed by name, bank account information, address and date of birth.

Driver licences and Medicare cards have also been found to be frequently targeted by identity criminals.

Cost of cybercrime and fraud

The true cost of cybercrime in Australia is a challenge to quantify as without mandatory data breach notification laws many incidents may go unreported.

The Identity Crime and Misuse in Australia 2013-14 Report released by the Australian Government's Attorney General's Department found that the cost of identity crime in Australia was approximately \$2 billion.

The components of this cost estimate were:

Cost of identity crime as a proportion of total fraud against the Commonwealth	\$28.5 million
Cost of identity crime as a proportion of total personal fraud	\$435 million
Cost of identity crime as a proportion of total serious fraud	\$149 million
Cost of identity crime as a proportion of total police recorded fraud	\$1.4 billion

The costs of preventing and responding to identity crime are estimated to be a further \$350m.

These cost of identity crime numbers are not exclusively credit cyber fraud, but Veda's experience is criminals engage in identity theft and falsification with the primary purpose of gaining a financial advantage, therefore credit is an attractive fraud target.

The Australian Payments Clearing Association (APCA) provides specific estimates of the cost of online fraud in relation to cards and cheques.

The APCA defines online fraud as "card-not-present"; in other words, non-face to face transactions. The cost of fraud is measured in cost per \$1,000 transacted on cards.

Payments industry data for 2014 show that fraud on Australian payment cards continues to increase in the card-not-present category, reflecting a global trend both in online card fraud and in cybercrime in general. Card fraud rates over the last year have grown from 46.6 to 58.8 cents for every \$1,000 spent.^{vii}

The APCA report found card fraud was costing Australia \$299.5 million a year (2014). Two thirds of this card fraud was occurring overseas (\$200.6 million).

As online and other forms of card-not-present commerce grow, so does the opportunity for fraud.

The report cites Reserve Bank of Australia data showing the proportion of card purchases made online, by telephone or mail order, represents nearly 25 per cent of the total value of debit card purchases and about 40 per cent for credit cards.

Figure Four: Trends in Cost of Card Fraud^{viii}
(Source: Australian Payments Clearing Association)

Fraud (\$m)	2009	2010	2011	2012	2013	2014
Card-not-present	\$90.6	\$131.2	\$198.1	\$183.1	\$210.4	\$299.5
Counterfeit/skimming	\$56.2	\$50.0	\$66.0	\$37.2	\$36.1	\$42.1
Lost/stolen	\$16.6	\$16.7	\$20.2	\$27.0	\$32.2	\$33.0
Never received	\$4.3	\$3.4	\$4.1	\$8.5	\$9.1	\$8.4
Fraudulent applications	\$1.8	\$1.1	\$1.1	\$3.5	\$1.5	\$1.2
Other	\$4.3	\$2.2	\$3.4	\$1.8	\$2.0	\$2.3
Total	\$173.7	\$204.5	\$292.8	\$261.1	\$291.4	\$386.6

US-based data protection researchers the Ponemon Institute says the average economic impact of cybercrime on Australian organisations increased from \$4.2 million last year to \$4.9 million per company^{ix} in 2015.

The study, which was sponsored by HP Enterprise Security, examined the costs incurred by 28 Australian organisations who were victims of cybercrime. Costs ranged from \$792,932 up to \$18 million.

From a consumers' perspective, the cost of credit fraud is more than lost money. The cost cited most by Australian consumers of the consequence of identity theft is the refusal of credit.

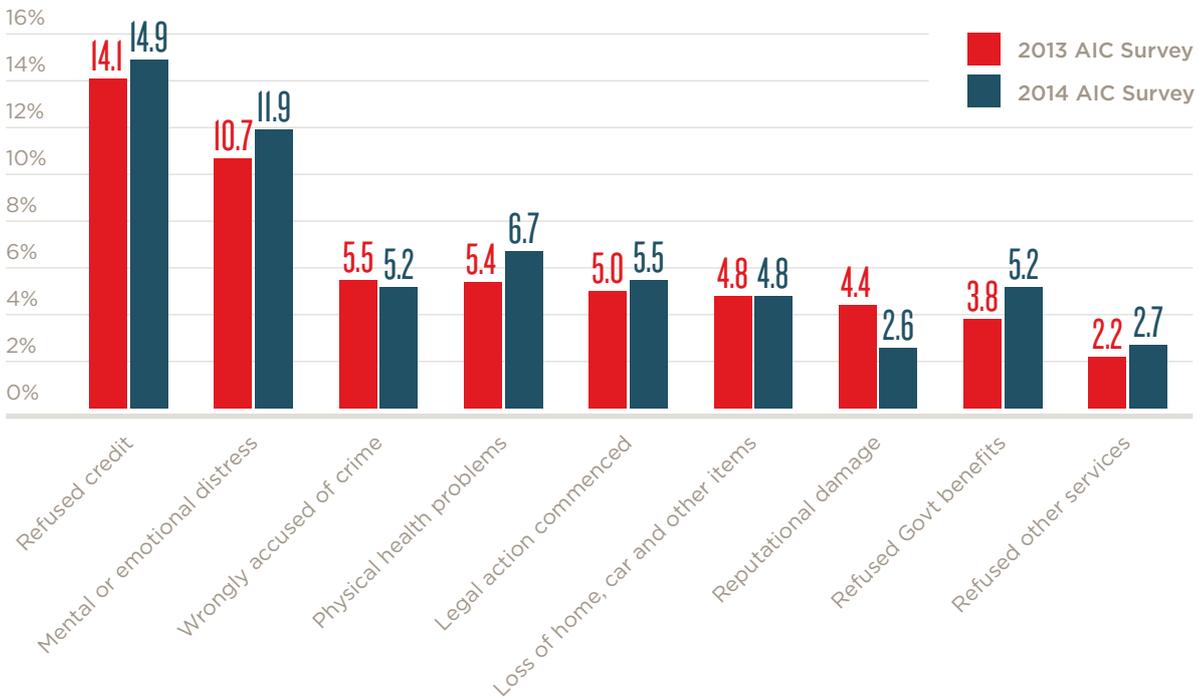
The 2014 AIC Surveys^x found that for people who had their personal information mis-used in the previous 12 months the top three consequences were:

14.9% refused credit

11.9% mental or emotional distress

6.7% physical health problems

Figure Five: Consequences experienced as a result of personal information being misused in the previous 12 months^{xi}
(Source: Australian Institute of Criminology)



Why criminals steal an identity

Criminals steal identities because they are seeking to use someone’s identity to conduct illegal activity, in many cases for financial gain.

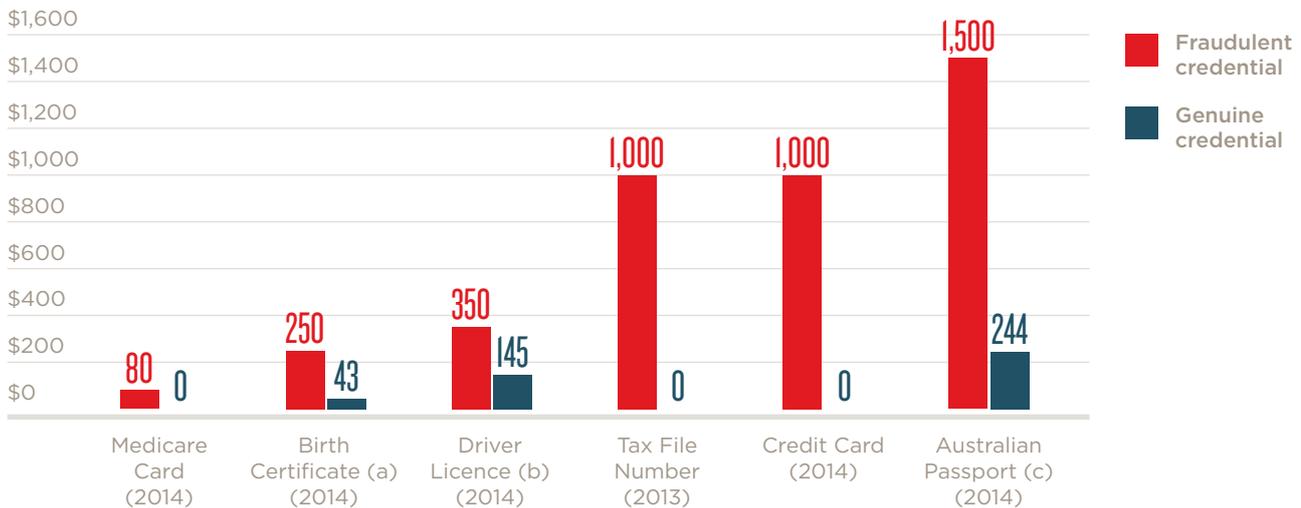
Australian Government agencies have published estimates for what it costs a potential fraudster to get hold of components of an individual identity or forged documents. A tax file number or credit card details retail in the underworld for \$1,000. It costs \$1,500 to have an Australian passport forged; this passport may be on-sold for between \$20,000 and \$30,000 on the black market.

Veda has a framework to help assist companies who have been victims of data breach. Veda continuously works on improving and developing a detailed understanding of not only how breaches occur but what the criminals do with the stolen information.

In a recent case a company whose employee system was breached received reports from over 20% of their employees that they had false tax returns filed in their name with funds being placed into a bank account unknown to them. In one case the tax return was valued at \$38,000.

Other than stealing money criminals also use individual personal information to conduct illegal activity. An example of this is leasing a property in someone else’s name. A criminal may conduct illegal activities from the property knowing that once they leave the property they are not able to be tracked as they have not used real personal information.

Figure Six: Price of fraudulent and genuine Australian identity credentials^{xii}
(Source: Australian Institute of Criminology)



- a. Based on fees for a standard birth certificate accessed from state and territory Offices of Births, Deaths and Marriages websites on 3 December 2014: \$42 (ACT); \$51 (NSW); \$30.20 (Vic); \$42 (QLD); \$44 (WA); \$43 (NT); \$46 (SA); \$45.88 (Tas).
- b. Based on fees for a 5 year licence renewal accessed from State and Territory Motor Vehicle Registry websites on 3 Dec 2014: \$167.10 (ACT); \$170 (NSW); \$154 (QLD); \$128.70 (WA); \$217 (SA); \$91 (NT); \$106.20 (Tas). The cost of a licence renewal in Victoria for 10 years is \$253.60. This figure was halved to reach a figure for five years (\$126.80). The average was then calculated.
- c. Cost to have a genuine passport altered by a professional document forger. A legitimately issued passport with fraudulent information retails for between \$20,000 and \$30,000 on the black market.

(Source: Australian Federal Police, Attorney-General’s Department and Department of Foreign Affairs and Trade)

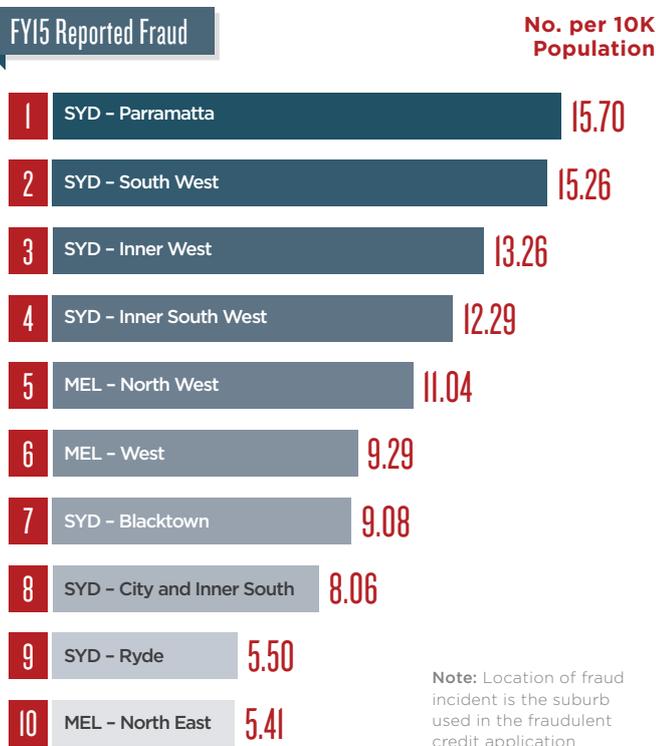
Where do the fraudsters come from?

In 2015, 55% of the addresses used in fraudulent credit applications were in Greater Sydney and Melbourne. The worst area per capita for fraudulent credit applications was Sydney's Parramatta, followed closely by South West Sydney. Outside Sydney, Melbourne's North West region ranked fifth worst nationally.

Figure Seven: Top 10 Areas for Fraudulent Credit Applications (Veda Shared Fraud Database 2015)

TOP 10 AREAS FOR FRAUD

55% of credit application fraud incidents were reported in Greater Sydney and Melbourne



While fraudulent applications for credit may be concentrated in Sydney and Melbourne, the impact on victims of credit application fraud does not respect state or national boundaries.

Veda's 2015 consumer survey found an even spread across the states and territories of people reporting they were the victim of fraud:



In the world of cybercrime the perpetrators can be from anywhere in the world.

5,106,804 notifications of malicious activity by programs designed to steal money via online access to bank accounts were registered by Kaspersky Lab security solutions in Q1 2015^{xiii}. Of these the following countries were the top 10 to be affected:

	Countries	Number of users attacked
1	Brazil	91,893
2	Russia	85,828
3	US	66,699
4	Germany	51,670
5	UK	25,269
6	India	22,085
7	Turkey	21,397
8	Australia	18,997
9	Italy	17,663
10	Spain	17,416

Consumer attitudes to cybercrime and identity theft

Each year, Veda conducts consumer research to gain insights into consumers' views and concerns about identity theft and other cybercrime.

In 2015, a survey of 1,024 Australians found:

6% of Australians report having being a victim of identity theft in the past 12 months

25% report they have been a victim of identity theft fraud at some stage

25% of victims of identity theft report they do not know how their information was stolen

The frequency of identity theft identified by the Veda survey is consistent with surveys carried out by the Australian Institute of Criminology. Surveys conducted in 2013 and 2014 found 9% of respondents experienced some form of misuse of their personal information in the previous 12 months, with approximately 5% of all respondents incurring out-of-pocket losses as a result of this misuse.^{xiv}

If identity theft and misuse is affecting between six per cent and nine per cent of Australians each year, this means between 1.4 and 2.1 million people are being affected annually by this insidious crime.

The level of identity fraud and subsequent credit fraud reported in Veda's consumer survey and in government surveys may under report the frequency of crime.

Many more people are likely to be unaware that their data had been stolen or compromised. Veda has been advised by global anti-fraud agencies that the time lag between information being stolen, and that information being used to steal, can be up to 12 months or longer. One US survey reveals that at least 15% of incidents are only discovered more than three years after the crime began.^{xv}

Figure Eight: Frequency of Identity Theft - Identity Theft in Australia and Australia's View of Personal Information Security Survey (Veda, 2015)

IDENTITY THEFT VICTIMS



1 in 4 (25%) Australians are aware of being a victim of identity theft or fraud at some stage

6% of Australians report having been **a victim within the last 12 months**

When it last happened:



1 in 4 (25%)

victims say they don't know **how** their information was stolen



There is an active global marketplace where criminals trade parcels of identity information to the highest bidder, or to a criminal who may wish to conduct a data match to improve their existing data and execute a large scale fraud event.

Australian's love of online commerce and sharing on social media makes them vulnerable to identity theft.

This has created a world of opportunity for cybercriminals who constantly vacuum up personal information online.

Australia's income levels and relative wealth of bank, credit card and superannuation accounts makes Australians an attractive target.

Clearly identifying how fraud occurs, the methods used and who the perpetrator was, is a difficult task, which requires many hundreds of hours of police work. Despite this Australian consumers believe a number of methods have been used to steal their information:

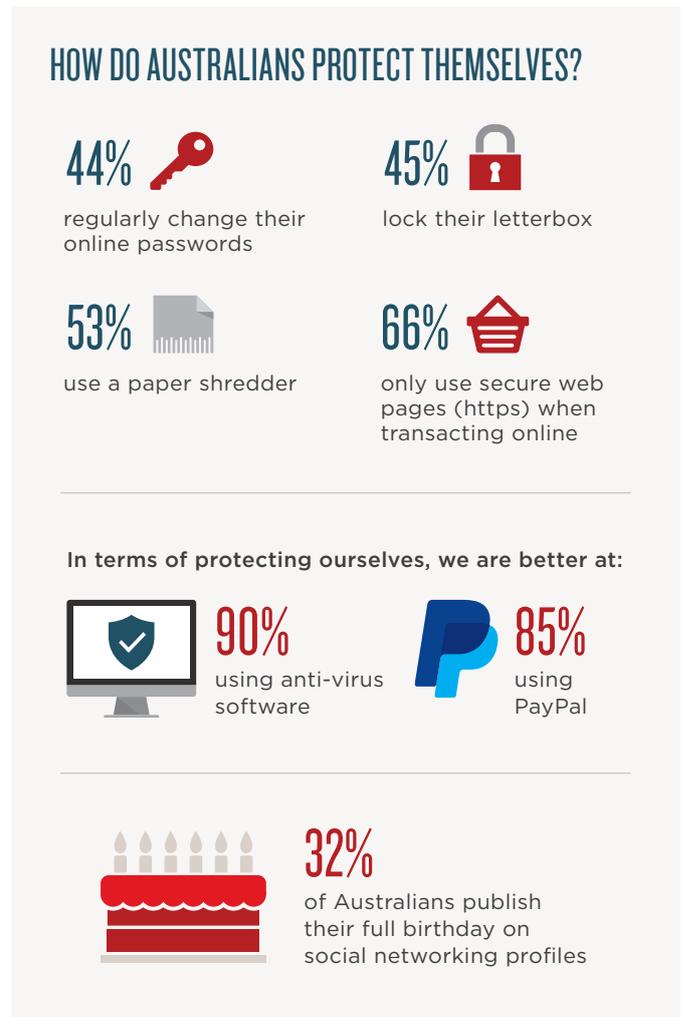
- 20%** of victims of cyber fraud reported their computers had been hacked
- 18%** reported their mobile phone had been hacked
- 18%** reported they had an online account or social media account hacked

Australians are becoming more concerned about cyber fraud and identity theft:

- 54%** are concerned about identity theft
- 70%** worry about putting their personal information online
- 61%** are uncomfortable giving out their credit card details online
- 71%** don't trust social media to protect their information

While respondents to the 2015 Veda consumer survey are concerned about identity theft, this does not necessarily translate to curbing their lax online behaviour. Astonishingly, fewer than one in two Australians (44%) regularly change their online passwords and only 66% use secure web pages (https) when transacting online. Almost one third (32%) of Australians publish their full birth date on social networking sites, which is a key piece of personal information used to verify someone's identity.

Figure Nine: How Do Australians Protect Themselves From Fraud? (Source: Veda)



Consumer attitudes to cybercrime and identity theft

The survey suggests that older Millennials, aged 26 to 29 years, are among those most at risk, with 35% claiming to be a victim of identity theft or fraud compared to 25% of all Australians. Yet the same group of Millennials believed their information to be very secure (32%), compared to all Australians (26%).

Figure Ten: Steps Australians Take to Protect their Identities from Cyber Fraud (Veda 2015)

What security measures do you put in place to protect yourself from identity theft?	October 2014	October 2015
Anti-virus software (e.g. Norton, McAfee)	86.2%	90%
PayPal online payments	81.2%	85%
Only use secure web pages (e.g. https pages when making online transactions)	69.2%	66%
Set social media to highest privacy settings	57.9%	55%
A paper shredder	50.9%	53%
Lock my post/letterbox	43.4%	45%
Change my online passwords regularly	No data	44%
Store passwords in a secure location/on a secure app	42.5%	40%
Use encrypted/secure email	41.8%	40%
Home safe to put important papers	24.7%	23%
Credit file alert	9%	9%

n = 1,000

As seen in the Veda study, many Australians are taking steps to protect themselves from identity theft, however it is important for us all to recognise that most traditional security controls can sometimes be bypassed.

Anti-virus software can be bypassed by criminals in the case of zero day attacks (attacks which no one knows about so anti-virus services cannot detect). Checking pages are secure may not always be failsafe if a criminal uses social engineering to trick the user into believing through messaging that they are safe. These security controls are still important but the ways criminals bypass these controls illustrates how important it is for Australians to continue to look for the newest technologies and ways to protect their identity. New technologies include personal information alerting services which let consumers know when your information is compromised but hopefully before they cause too much damage.

As fraudsters get more sophisticated, consumers need to get smarter about how they protect their personal information such as passwords, personal details and financial information.

Data breaches

In 2014/15, the Office of the Australian Information Commissioner^{xvi} reported the highest ever number of notified data breaches in Australia; 117.

A data breach is defined as when personal information held by an agency or organisation is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.

A data breach does not involve just a single consumer having their identity compromised; it involves the unauthorised access of hundreds, thousands and sometimes millions of records containing personal information.

At least one data breach occurs every week in Australia, with an average of 20,073 records lost or stolen per incident^{xvii}.

In Australia, there are currently no laws requiring mandatory reporting of data breaches by organisations.

Proposed privacy laws are expected to compel organisations to report breaches of customer data, imposing stronger obligations on businesses to respond to hacking, stealing or accidental release of personal information.

Currently, the true scale of data breaches in Australia is unknown due to the lack of notification laws. Overseas experience suggests that unreported data breaches are far more common than people impacted are aware.

New data breach notification laws would give affected individuals a better chance to protect themselves from further damage should their personal data be released.

A Veda analysis of global information privacy laws in 53 developed countries showed that in 54% of countries, there are laws mandating that companies notify individuals in the event of a data breach. In 36% of the countries, companies are required to go a step further and advise individuals what to do to protect themselves.

Tightening up the privacy law in Australia would encourage organisations to improve their data handling practices to protect both themselves and their customers from reputational damage, financial losses and the growing threat of data breach.

A Veda survey of 1,000 Australian consumers in September 2015 found that 79% believed that corporations should have to tell them if their data has been compromised from a breach.

Of this group who expected compulsory notification, 33% believed corporations should provide advice on how consumers should protect themselves as result of a breach and offer an identity protection alert service to minimise risk post-breach.

A 2014 survey conducted by the US based Identity Theft Resource Centre revealed that of respondents who received data breach notification letters, the following follow-up activities had been performed:

45% contacted their financial institution

44% contacted the organisation that sent the notification

41% requested a credit report

34% enrolled in the free credit/identity monitoring which was being offered^{xviii}

Data breach **case study** of online retailer

In October 2015 an Australian online retailer was the victim of cybercrime and as a result had 12,000 of its customer records compromised.

The company was quick to act and provided impacted individuals with credit monitoring and identity protection services which helped affected individuals retain trust in the brand and allowed the individuals to take action to protect themselves from further harm. This type of action from a company is often applauded by the privacy and security community and even more so by customers. In other markets like the US this type of action by a company is not only mandated by law but also a response expected by the individuals impacted.



Data breach **case study** of an insurance company

In late October 2015 an Australian insurance company had their accounting system compromised.

By accessing the system criminals were able to collect a variety of personal information including the payroll details of all the companies' employees. Within days the criminals used this information to log into a government website where they promptly changed the employees' bank details for tax returns and lodged false tax returns in the employees' names.

Over 20% of employees had false tax returns filed in their name with the resulting financial benefit deposited to an unknown bank account. This shows a planned and sophisticated attack by criminals who knew which systems they needed to access in both the company and the government to get the desired outcome.

All employees were provided credit and identity protection services by Veda and the feedback was extremely positive. Many employees were thankful to their company for doing everything they could and found the honest communication a positive experience.



Combating cyber fraud

Evolving technology

Fraud prevention online needs to continually improve and respond to evolving criminal technology.

There is no one silver bullet to ensuring personal or company information is not at any risk. As the banks have known for many years a multi-layered approach to implementing security practices is required for maximum effectiveness.

Second factor authentication needs to continue to be deployed for all systems holding personal information.

As seen in the biggest banking breach in history all it takes is for one employee to be compromised and for that company to have one server without appropriate security controls for criminals to gain access.^{xix}

A recent study by Verizon mapped critical security controls to incident event chains and ended up with a top 14 list of security controls. Verizon went as far as to document the percentage of incidents where this control could be applied as the recommended strategy.^{xx}

Figure Eleven: (Source: 2015 Verizon Data Breach Investigation Report)

Description	Percentage	Category
Two factor authentication	24%	Visibility/attribution
Patching web services	25%	Quick win
Verify need for internet facing devices	7%	Visibility/attribution
Proxy outbound traffic	7%	Visibility/attribution
Web application testing	7%	Visibility/attribution
User lockout after multiple failed attempts	5%	Quick win
Block known file transfers	5%	Advanced
Mail attachment filtering	5%	Quick win
Limiting ports and services	2%	Quick win
Segregation of networks	2%	Configuration/hygiene
Password complexity	2%	Visibility/attribution
Restrict ability to download software	2%	Quick win
Anti-virus	2%	Quick win
Vet security process of vendor	2%	Configuration/hygiene

40% of these controls fall into the quick win category showing us that not all security controls are entirely complex and time consuming to set up.

People power

Cybercrime has been around since the beginning of the internet when in 1978 the first spam message was sent. Many early threats relied on problems with technology; loop holes in operating systems or browsers through which criminals could take advantage.

As more and more software providers establish robust security features, criminals are increasingly turning towards social engineering tactics which involve tricking humans into being a part of the cybersecurity problem.

From clicking on phishing emails, propagating viruses in internet posts or being interested in advertising with malware (malvertising) humans are the weakest link in the most robust security practices.

Veda's 2015 research shows that Australians are more interested in being part of the solution than ever before with 95% of people doing something to protect their identity - up 9% since 2014.

Getting customers and employees really engaged in preventing security breaches is the only way organisations can ensure their security policies are as robust as possible. As Symantec has suggested^{xxi} the security industry gamifying security so that it is more interactive and fun will engage the younger, more lax generation.

Veda's role in combatting cybercrime and fraud

Credit file and personal information alerts

Veda offers credit file alerts so subscribers are notified if anyone applies for credit in their name. An alert would be triggered by a criminal attempting to apply for credit in someone else's name allowing the subscriber to take immediate steps to stop the fraud.

Veda's Identity Watch service is a cyber-monitoring product, used to help detect fraud by constantly looking for information - such as credit and debit card numbers, phone numbers and email addresses - in places on the internet where information is known to be illegally traded.

Identity Watch subscribers provide the information they would like monitored, such as credit or debit card numbers, phone numbers and email addresses. Veda stores this information securely and uses tools such as web crawlers and forum extraction to locate compromised data online.

If Identity Watch finds that an identity-monitored item has been compromised, it will automatically send an email alert so the subscriber can take action.

While Identity Watch is available for individual consumers, Veda also offers Identity Watch to corporate partners who may wish to include Identity Watch in offers to employees, customers, or as amelioration in the event of a data breach.

Data breach support and remediation

Veda plays a critically important role in assisting organisations and individuals recover from the increasing number of data breaches. Veda provides credit and identity protection services to organisations and individuals affected by this type of cybercrime.

There is an opportunity to intervene after a data breach has occurred and before criminals have the opportunity to use stolen data to commit fraud. Veda's credit file and personal information alerts are key tools for this type of remediation.

Veda is leading the way in data breach response planning by working not only directly with affected organisations and individuals but also with insurance companies and legal bodies who play advisory roles during these incidents.

Veda provides leading edge consumer identity protection services to many Australians who are concerned about online crime and are looking for ways to feel safer while online. Information about these customers informs Veda's view on how fraud impacts Australians.

1 in 4 Australians have been a victim of identity theft^{xxii}

79% of Australians believe organisations should notify them if their data is lost or stolen^{xxiii}

Shared Fraud Database

Veda plays an important role in combatting cybercrime and fraud by operating the Shared Fraud Database, a repository of insights from Australia's leading credit providers about fraudulent activity.

Members of the Shared Fraud Database are known as the Veda Fraud Focus Group. Australia's 'big four' banks, international financial institutions, telecommunications providers, motor vehicle financiers and other credit providers such as credit unions and asset financiers, all contribute and benefit from data in the Shared Fraud Database. The Fraud Focus Group offers a collaborative, knowledge-sharing service that helps members identify fraud at the point of application and before substantial losses can occur.

Veda's Shared Fraud Database is an important resource in Australia's efforts to combat cybercrime. Members who are invited to join Veda's Fraud Focus Group have access to a database of confirmed fraud events as well as additional intelligence material highlighting trends, patterns and market insights. By sharing data on known fraudsters and methods of fraud, members of the Shared Fraud Database have collective strength.

Each year, Veda identifies approximately \$1 billion in fraudulent credit applications.

Fraudsters can be banned from applying for credit, devices used for previous fraudulent applications can be red-flagged and strategies and products to remain one step in front of fraudsters are continuously being developed.

Identity verification

Veda developed the IDMatrix technology to provide companies and government agencies an online solution to verifying an individual's identity.

Veda's IDMatrix electronically verifies identity details at the point of application – whether that be online, face-to-face, in a retail setting, or through a call centre or back-office processing centre. In a matter of seconds, Veda's system will search through up to 22 independent database sources. This provides organisations of all sizes with the ability to immediately verify a customer's identity without relying on the sighting of paperwork and ID documents.

Knowledge Based Authentication (KBA) is a feature of IDMatrix designed to present out-of-wallet questions. An out of wallet question is literally information that cannot be found in a stolen wallet or easily discoverable online. The system asks dynamically generated questions only the applicant should know. KBA ensures the person claiming an identity is indeed that person.

In the property sector Veda provides tenancy screening services to real estate agents across Australia so they can identify if their prospective tenant is blacklisted and verify if the documents provided to the real estate agent are genuine.

Employee background screening

A potential risk to organisations is employing an individual who is a criminal, or has links to criminals and intends to steal information to commit fraud.

Veda's Verify service offers up to 75 separate checks on current or potential employees. These checks include identity, criminal background checks, qualification and registration, credit and licence checks.

Carefully screening employees addresses another potential fraud risk point.

Device intelligence

People connect to online business with all kinds of devices, including smartphones, tablets, laptops and notebooks. No matter what the platform, the customer or website visitor's device can present the weakest link in cyber security.

Device intelligence technologies can help reveal people who are not who they claim to be. Veda's device fraud service developed by ThreatMetrix and licensed to Veda in Australia, is a cloud-based, real-time device identification and identity verification solution. It helps to protect businesses against cyber criminals and validate returning customers and prospects.

The service provides patented VPN detection capability, which determines the true nature of hackers who are trying to hide their device identity and location. The system screens transactions against a global database of over 60 million known fraudulent devices. The Veda system provides organisations with the insights required to determine whether to proceed, challenge or prevent an online transaction.

Veda provides these products and service to the business, government and consumer market and Veda's fraud and cybercrime teams are always looking for ways to help both markets deal with the ever increasing threat of cybercrime.

Looking ahead – cybercrime and fraud in 2016

In this section, Veda looks ahead to some of the key cybercrime trends and challenges for 2016.

- 1 Cybercriminals will become more interested in the health sector due to the wealth of data held by healthcare organisations and a perceived weakness in their cyber defences.
- 2 Emboldened by successful data hacks into on-line retailers over the past two years, cybercriminals will continue to target the retail sector, with a particular focus on new to online retailers and main street retailers who are building an online retail channel.
- 3 The Privacy Act will be amended to put the onus on organisations that suffer data breaches to notify the Privacy Commissioner and the individuals affected, particularly if the breach is seen as a 'serious data breach' where there is a real risk of serious harm to the individual or if the information released was particularly sensitive, such as health records.
- 4 Consumer expectations will continue to grow for direct action to be taken by organisations responsible for the breach of their valuable personal information. Consumers will want information, guidance and tools to protect their identity, not just notification of an internal IT security fix.
- 5 As more and more services move to verifying documents using central services such as the government document verification service, criminals will begin to step up their game to get past these controls and additional verification services to validate other aspects of identity will be needed.
- 6 The Internet of Things means that more and more 'things' (phones, vehicles, wearables) are becoming interconnected. Data is being recorded on an increasingly unfathomable scale and this trend is set to continue. Significant concerns from consumers relating to service providers limited security features, and the potential for invasion of privacy will need to be addressed.
- 7 Crime within social media will rise as seen by the growing number of new threats like jacking, fake apps and malvertising. Criminals will increasingly rely upon unsuspecting humans to be a part of their overall game plan.
- 8 Ransomware campaigns, where malware encrypts files so that a computer or specific files cannot be accessed until a ransom is paid, will become more prevalent in Australia.
- 9 With the increased use of government document verification systems being used to validate documents, criminals will increasingly require real identities to pass verification checkpoints. This will see rise in the sophisticated and complex ways in which criminals will go about collecting detailed personal information about real individuals.
- 10 The number and sophistication of cybercrime attacks on individuals, firms and government agencies, will continue to increase.

For more information

To find out more about the information in this report and cybercrime in Australia please get in contact with Veda's cybercrime team.

Email: identitywatch@veda.com.au

Visit:

veda  **Identity Watch** identitywatch.com.au

veda  **YOUR CREDIT AND IDENTITY** veda.com.au/yourcreditandidentity

secure  **sentinel**
Part of the Veda Group secaresentinel.com.au

veda  | **IDMatrix** idmatrix.com.au/about

veda  veda.com.au/business/fraud-prevention/device-intelligence

 **verify**
Part of the Veda Group veda.com.au/business/verification/verify

Sources

- i. Australian Cyber Security Centre 2015 Threat Report 2015, p 5. acsc.gov.au
- ii. Veda Shared Fraud Database 2014/2015
- iii. Identity Crime and Mis-use in Australia 2013-14; Attorney General's Department, p 8. ag.gov.au
- iv. Veda Shared Fraud Database 2014/15
- v. As above
- vi. Identity Crime and Mis-use in Australia 2013-14; Attorney General's Department, p 50. ag.gov.au
- vii. <http://www.apca.com.au/docs/fraud-statistics/Australian-payments-fraud-details-and-data-2015.pdf>, pg 2
- viii. Australian Payments Fraud: Details and Data. Australian Payments Clearing Association 2015, p 9. apca.com.au
- ix. Ponemon Institute 2015 Cost of Cyber Crime Study. www8.hp.com/au/en/software-solutions/ponemon-cyber-security-report/
- x. Australian Institute of Criminology Survey, cited in Identity Crime and Mis-use in Australia 2013-14; Attorney General's Department. ag.gov.au
- xi. As above
- xii. As above
- xiii. <https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/>
- xiv. Identity Crime and Mis-use in Australia 2013-14; Attorney General's Department, p 4. ag.gov.au
- xv. Identity Theft: The Aftermath 2014™ Conducted by the Identity Theft Resource Center® (ITRC), p 22
- xvi. <https://www.oaic.gov.au/media-and-speeches/media-releases/annual-report-2014-15-working-with-government-business-and-communities-to-protect-australian-privacy>
- xvii. Identity Crime and Misuse in Australia. Australian Attorney-General's Department. September 2015 <https://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/Identity-Crime-and-Misuse-in-Australia-2013-14.pdf>
- xviii. Identity Theft: The Aftermath 2014™ Conducted by the Identity Theft Resource Center® (ITRC), p 30
- xix. <http://arstechnica.com/security/2014/08/jpmorgan-other-banks-hacked-and-fbi-looks-to-russia-for-culprits/>
- xx. 2015 Verizon Data Breach Investigation report, p 56
- xxi. Symantec Internet Security Threat Report 20, April 2015
- xxii. Veda Commissioned Survey. The Leading Edge: Survey of 1000 Australian Adults, September 2015
- xxiii. As above

© Veda Advantage Information Services & Solutions Ltd. No part of this document may be reproduced without the prior written permission of Veda Advantage Information Services and Solutions Ltd.

This summary, the service described and related product collateral do not constitute legal or compliance advice. Organisations are encouraged to obtain independent legal advice.

To find out more visit veda.com.au