VEDA 2016

Cybercrime and Fraud Report

veda

An Equifax Company

Contents

02 **Introduction**

03 **Report Summary**

04 **Cybercrime and Fraud in 2015 – A Year in Review**

05 **Cybercrime and Fraud in 2016**

07 Where does Fraud occur?

08 **How Cybercrime and Fraud affects Business and the Economy**

11 **Consumer Attitudes to Cybercrime and Identity Theft**

12 **Future Challenges – Cybercrime and Fraud in 2017**

13 **Combatting Cybercrime and Fraud**

13 Protecting Businesses

13 Protecting Individuals

14 Veda's Role in Combatting Cybercrime and Fraud

Introduction

Veda is a data analytics company and the leading provider of credit information and analysis in Australia and New Zealand. From its core credit bureau business established in 1967, Veda has expanded to deliver a suite of credit and other analytical products targeted to customers and specific industry segments.

Veda's customers use data intelligence provided by Veda to make decisions on credit risk, verify identity and employee backgrounds, reduce identity theft and fraud, and undertake digital marketing strategies.

In February 2016, Equifax Inc., a global leader in information solutions, finalised its acquisition of Veda. Equifax powers the financial future of individuals and organisations around the world, using its combined strengths of unique trusted data, technology and innovative analytics. Together, Veda and Equifax offer their customers world-leading insights and knowledge to help them make informed decisions.

Veda works in the fraud and online security sector alongside Australian businesses, government departments, enforcement agencies and individuals, providing insights and analysis to develop anti-fraud solutions. This work gives Veda deep insights into cybercrime and fraud.

Last year, Veda compiled valuable insights from its work in the fraud and online security space to create the first annual **Cybercrime and Fraud Report**. The report offered a deep-dive into the established and emerging trends in cybercrime and fraud in Australia in 2015.

This year's report is a summary of the latest information and insights from Veda, offering an understanding of cybercrime and fraud in 2016 and beyond.

The dual threats of cybercrime and fraud in Australia have continued to grow in the 12 months since the 2015 Cybercrime and Fraud Report was released, evolving at speed to keep one step ahead of businesses and consumers.

The most common types of cybercrime reflect the personal and professional lives of Australians in 2016. Given the increasing use of online channels for business, socialising and communication, it follows that these channels also offer the most rewarding opportunities for cybercriminals.

Phishing scams, card-not-present fraud involving the buying or selling of goods online, social hacking and company data breaches are fast becoming criminals' livelihood as they look for ways to access and leverage private information for their own profit.

Unsurprisingly, the credit industry is a particularly high profile target for cybercriminals because of the potential direct access to financial gain.

However, it is important to remember that stealing personal information from individuals allows criminals to do more than just steal or launder money; they may also defame, blackmail or expose sensitive facts about individuals or corporations. In some of the most serious cases of complete identity takeover, a cybercriminal may even succeed in creating an entirely fabricated life through credit transactions, causing major losses to lenders and financial institutions, making it difficult to repair the credit history of their victim.

This report provides insights into the frequency, types and trends of cybercrime and fraud in 2016, and details the impacts on individuals and businesses. The information is drawn from exclusive data from Veda's Shared Fraud Database, insights from Veda consumer research, and data from specialist government and industry bodies.

It is a useful resource for any organisation or individual who may be the target of cyber fraud and wants to know more about how to protect themselves and their assets against this ever-present threat.

> "On the evidence available, it is clear that the number, sophistication and impact of cybercrime continues to grow and poses a serious and evolving threat to Australian individuals, businesses and governments."[i]
>
> **Australian Government's National Plan to Combat Cybercrime**

Report Summary

Key Findings

Reported volume of online credit application fraud incidents by Veda Fraud Focus Group members
up 33% in FY2015/16 compared to FY2014/15

57% of credit application fraud
in Australia is now occurring online

Identity takeover is the fastest growing type of fraud,
up 80% in FY2015/16 compared to FY2014/15

27% year-on-year increase
in falsifying personal details

More than a quarter of all Australians (27%)
have been a victim of identity theft

Cybercrime and Fraud in 2015 – a year in review

The four main sub-types of credit application fraud considered in Veda's Cybercrime and Fraud Report are:

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

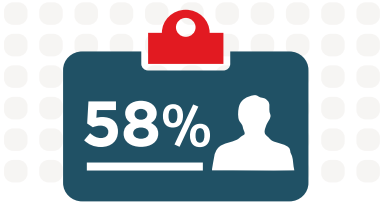
In 2015, Veda's Cybercrime and Fraud report showed that:

- **25% of Australians** had been a victim of identity theft, **up 17% year-on-year**
- **50% of all credit application fraud** in Australia was occurring online
- Fraudulent credit applications involving identity takeovers had **risen 59%** in the previous two years

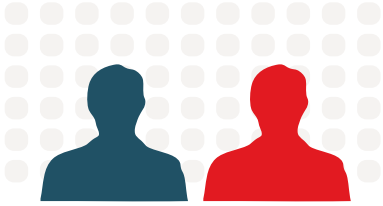
The 2015 report also revealed that identity takeovers were increasing, but that falsifying personal details remained the most common attempted type of credit fraud, making up 58% of total credit application fraud incidents (see Figure One).

Types of credit application fraud incidents

growth in **identity takeovers** in the past year



are due to **falsifying personal details**



Doubling of **fabricated identities** in the past year

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

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

Cybercrime and Fraud in 2016

The latest insights from the Veda Shared Fraud Database reveal that the incidence of fraud shows no signs of slowing in 2016. The volume of reported fraudulent activities climbed 33% year-on-year from FY2015 to FY2016.

Unsurprisingly, the volume of fraudulent credit applications occurring online has risen once again. Reports of fraud through online channels make up 57% of all fraudulent applications in the six months to June 2016 (see Figure Three), up from 50% in the same period in 2015, and 45% in 2014. This upward trend in online fraud is likely to continue into the future, as individuals and businesses become ever more reliant on the internet for their banking, shopping and other financial interactions.

Another continuing trend is the growth of **identity takeover**, where a genuine identity is stolen from an individual and misused for financial gain. This type of fraud goes hand-in-hand with data breaches, as these incidents give cybercriminals access to the details they need to steal a person's identity.

Identity takeover is growing faster than the average across fraud types – up 80% in FY2016 – and is second in frequency only to **falsifying personal details**. This remains by far the most common fraud type, accounting for almost 71% of all reported fraud incidents (see Figure Two). Falsifying personal details increased 27% in FY2016, and has grown consistently over the past three years. Falsifying personal details includes fabricating or altering pay slips, tax assessments and bank statements.

For fraudsters seeking to cash in on falsified personal details, payslips were the most common target by a large margin. Bank statements and drivers' licences were also highly ranked falsified documents, suggesting a continued trend towards falsifying income, which was also the case in 2015.

Falsified payslips were the most commonly used documents in cases of attempted identity takeover – a change from the 2015 report, when drivers' licences were the most common document put forward by criminals looking to perpetrate this kind of fraud.

Payslips were closely followed by documents such as drivers' licences, bank statements and utility bills. Some of these documents are considered to be more accessible to criminals, as they are left unattended for hours or even days in unlocked and unguarded letterboxes. This may change, however, as more banks and utility providers encourage the use of online statements.

In cases of fabricated identity, drivers' licences were the most commonly reported document by a high margin.

Fraud Type % of Total Fraud

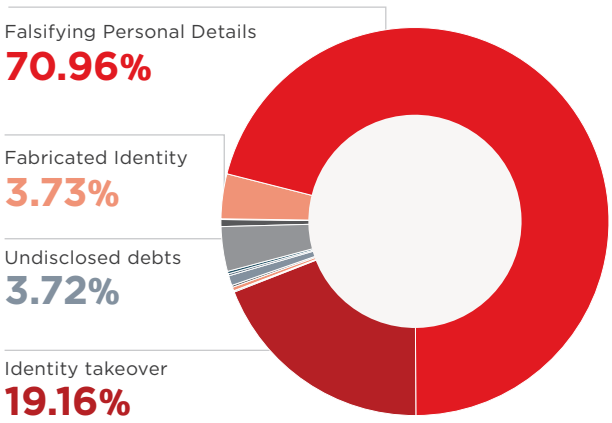


Figure Two: Proportion of Fraud Sub-Types as a % of all confirmed fraudulent credit applications[iii]

Channel source of fraud

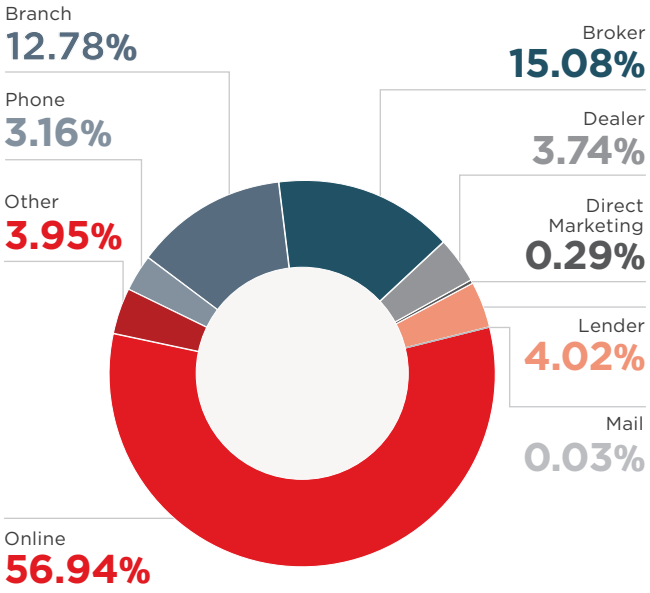


Figure Three: Channel source of fraud as a % of all fraud[iv]

Cybercrime and Fraud in 2016

While **online credit application fraud** remains the most common form of credit application fraud in 2016, growth in fraud through the broker channel is an ongoing concern. Broker channel fraud makes up 15% of all credit application fraud (see Figure Three), and has grown a significant 25% in H2 FY2016.

Fraudulent credit applications through branches, which fell in 2015, experienced a resurgence in 2016, rising 13%. This may be a result of continued use of manual processes which often involve a high level of subjectivity when verifying identities.

Consumer credit cards were the target of the majority of fraudulent credit applications in 2016, representing 45% of all credit fraud reported on the Veda Shared Fraud Database (see Figure Four). Despite this significant majority, the share of fraud attributed to consumer cards has decreased in the past 12 months.

Although the proportion of fraud reported on consumer cards decreased, this was not due to a decline in fraudulent card activity. Instead, the proportional balance was shifted by the considerable upswing in **telecommunication product fraud**, which accounts for almost 9% of all fraud reported to the Shared Fraud Database in 2016 (see Figure Four), up from 1% of total fraud in 2015.

This increase is due to improved fraud detection techniques amongst telecommunication companies. These techniques have an ongoing compounding effect; data from confirmed fraud cases plays a key role in detecting subsequent attempts.

Fraudulent **personal loan** applications represented 16% of total fraud, while fraudulent **mortgage applications** also made up a significant proportion of total fraud, with 13% (see Figure Four).

Falsifying personal details was the most common fraudulent activity for all the major fraud types by product, including consumer credit card, telecommunication product, personal loan and mortgage application fraud.

Product type % of total fraud

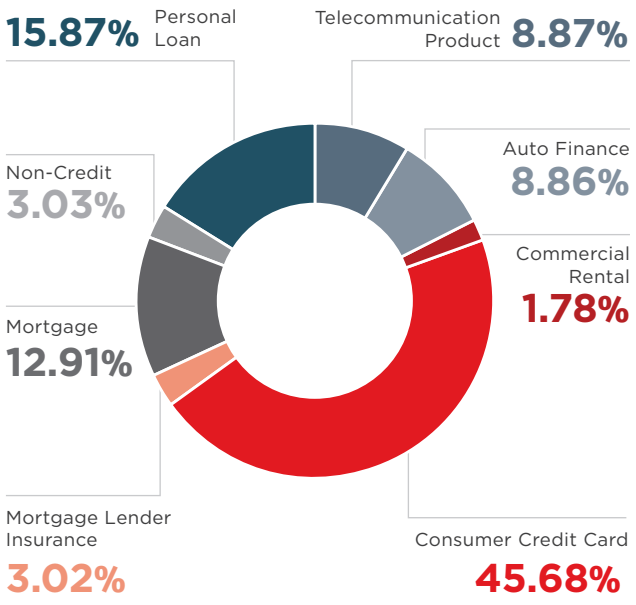


Figure Four: Product type % of total fraud[v]

WHERE DOES FRAUD OCCUR?

In 2016, 72% of all fraud incidents were reported in Greater Sydney and Melbourne. The highest rate of fraud per capita for fraudulent credit applications for the second year running was Sydney's Parramatta, followed closely by South West Sydney. Melbourne's North West region came in as the third worst area for fraudulent activity nationally (see Figure Five).

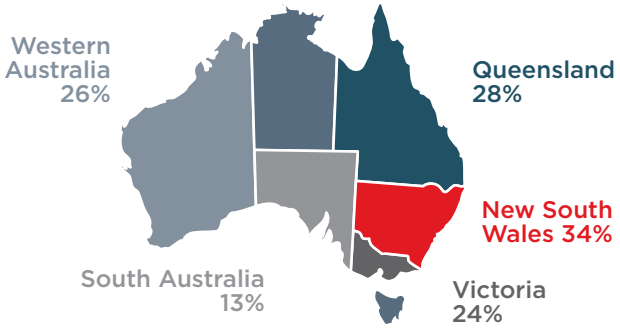
High population density and the relative anonymity experienced in capital cities make them a hotbed of opportunity for criminals.

However, much of the growth in fraud is occurring outside these metropolitan hotspot areas. In 2016, Newcastle and Lake Macquarie, Richmond – Tweed, and Baulkham Hills and Hawkesbury proved to be the fastest growing areas for fraud (see Figure Six).

It is important to note, however, that the place in which a fraud incident is reported may not be the same area the victim lives in. Fraud is most often reported in the location where the crime was perpetrated; for example, near to the address used to apply for credit with an assumed identity.

In many instances, fraudsters will steal the details they need from their victim, but return to their local area before using the stolen information. In other cases, the fraud victim may be travelling when the fraud incident happened, or may not have realised their information had been compromised until they were in a new location.

Veda's 2016 consumer survey found that people who had been the victims of identity theft are distributed relatively evenly across all states and territories:



Top 10 areas for fraud per capita

Rank	Area	H2 FY16 Incidents per 10K capita
1	Sydney - Parramatta	12.32
2	Sydney - South West	9.29
3	Melbourne - North West	7.99
4	Sydney - Inner South West	7.86
5	Sydney - Inner West	7.59
6	Sydney - City and Inner South	6.05
7	Sydney - Blacktown	5.82
8	Melbourne - West	5.68
9	Melbourne - Inner	4.68
10	Sydney - Ryde	4.11

Figure Five: Top 10 Areas for Fraudulent Credit Applications[vi]

Fastest growing areas for fraud

Rank	Area	H2 FY16 Incidents	% Growth HoH
1	Newcastle and Lake Macquarie	53	130%
2	Richmond - Tweed	25	127%
3	Sydney - Baulkham Hills and Hawkesbury	38	111%
4	Illawarra	42	100%
5	Wide Bay	23	92%
6	Brisbane Inner City	55	72%
7	Australian Capital Territory	37	68%
8	Sunshine Coast	30	58%
9	Perth - South West	36	57%
10	Geelong	64	56%

Note: Areas excluded where less than 20 incidents reported in 2016

Figure Six: Fastest Growing Areas for Fraud[vii]

How Cybercrime and Fraud affects Business and the Economy

The cost of cybercrime to the Australian economy has previously been estimated at more than $2 billion, as reported in the Identity Crime and Misuse in Australia 2013-14 Report by the Australian Government's Attorney General's Department.

However, it is widely understood that the true cost of cybercrime is difficult to pin down, due to factors including Australia's absence of mandatory data breach notification laws.

In 2016, the average cost of a data breach to a company was $2.64 million.[viii]

The Australian government believes that, to be competitive and keep up with the changing habits of consumers, businesses need to be online. But by becoming a bigger player in the online marketplace, Australia may also be an increasing target for cybercrime and espionage.[ix]

According to the Australian Cyber Security Centre's 2015 Cyber Security Survey, half of all major Australian businesses experienced at least one cyber incident in the past year, and 56% of survey respondents have increased expenditure on cyber security in the past 12 months.[x]

The increased spending primarily went towards new technical and procedural controls, obtaining vulnerability assessments and compliance audits.

In its annual data breach study, US-based data protection researcher, the Ponemon Institute, revealed that the most common – and costly – cause of data breaches in Australia in 2016 was a malicious attack[xi] (see Figure Seven).

These attacks far outstripped the number of breaches caused by genuine **system glitches** or **human error**.

Malicious attacks may be orchestrated by either external hackers or criminal insiders. They can take any number of forms, from ransomware and malware incidents, to theft of physical devices or unauthorised access to information by staff, to denial of service attacks.

Online fraud in relation to consumer credit and debit cards is also on the rise.

The rate of fraud across all Australian cards and cheques, which is measured per $1,000, increased 18% year-on-year in the 12 months to December 2015, according to the Australian Payments Clearing Association (APCA).[xiii]

In the same period, more than $469 million worth of transactions on Australian cards were fraudulent.

While the APCA measures fraud across payments by cards and cheques, the rate of fraud associated with cheques is relatively insignificant. The total rate of cheque fraud in the 12 months to December 2015 accounted for less than 1% per $1,000.[xiv]

These figures reflect the increasing digital payment habits of Australian consumers, who spent 5% more on cards in 2015 than in 2014. In contrast, cheque use has dropped 70% over the past 10 years.

The fraudulent activity measured by the APCA occurs in two main categories:

- **Card-Not-Present** (CNP) fraud, which is when valid card details are stolen and used to make fraudulent payments
- **Card-Present-Fraud**, which is when a card is used fraudulently in a physical transaction, such as at an ATM or point-of-sale

CNP fraud is driving the overall increase in card fraud. This type of fraud increased 38% in 2015, making up 79% of all card fraud perpetrated (see Figure Eight).

This can be linked to the continued growth of online retail transactions taking place in Australia, and the fact that chip technology in debit and credit cards makes it harder for cybercriminals to perpetrate card-present fraud.

In cases of CNP fraud, cybercriminals often use malware to target the computer systems of retailers or service providers to capture stored card details, or target individuals through phishing campaigns.

Root causes of data breach

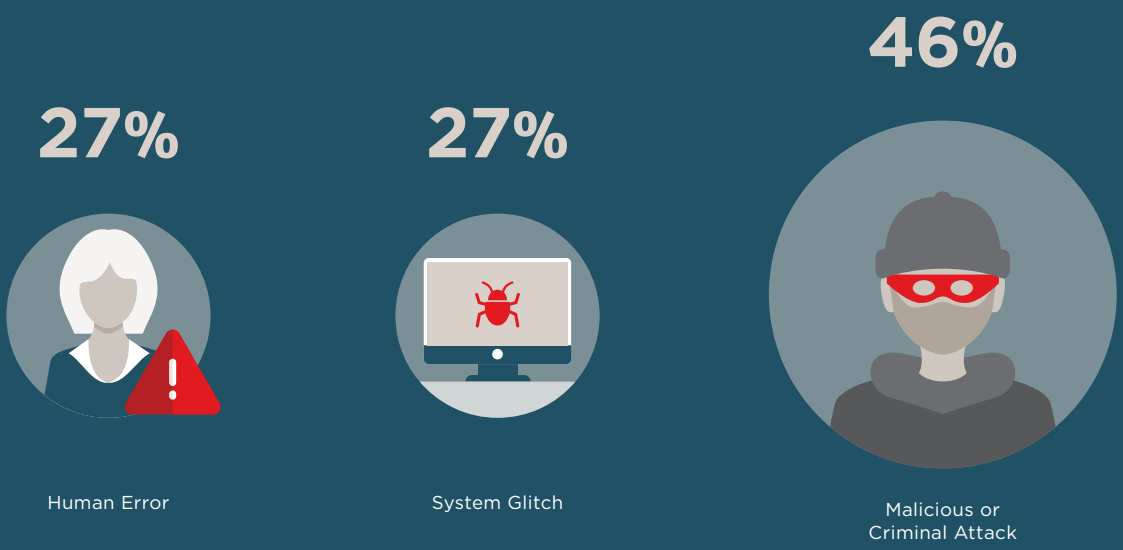


Figure Seven: Root Causes of Data Breach[xii]

Fraud type % of Total Card Fraud

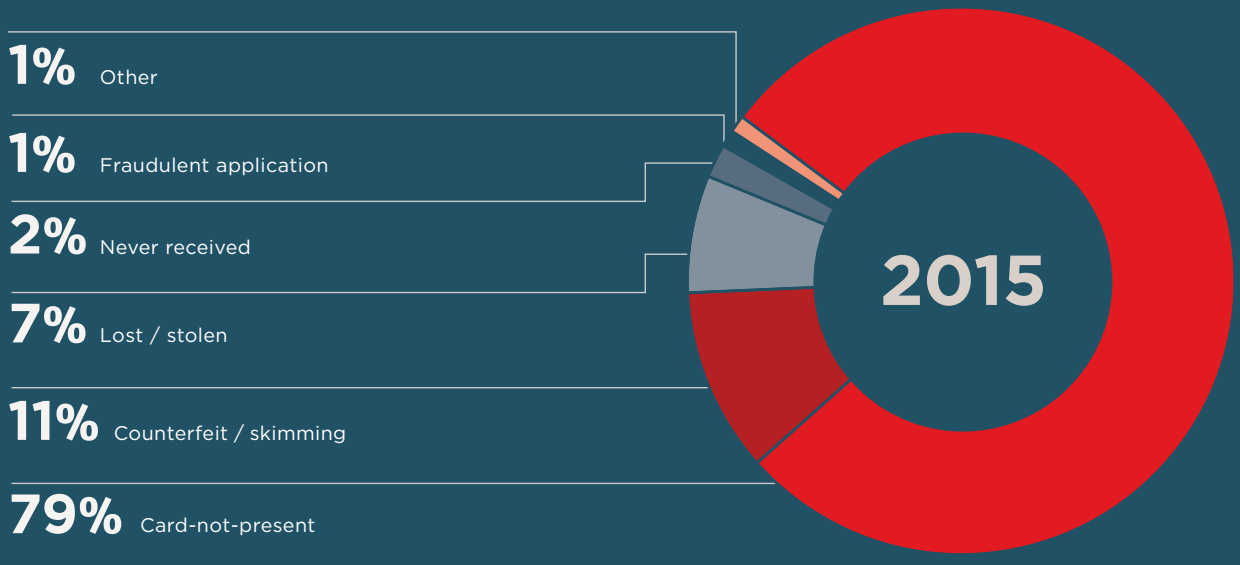


Figure Eight: Fraud Type % of Total Card Fraud[xv]

Most to least prevalent forms of fraud

1. Phishing / Email Scams
2. Debit or Credit Card Skimming
3. Malware or Computer Viruses
4. Identity Theft
5. Social Media Account Hacking
6. Medical Record Theft

Figure Nine: Most to Least Prevalent Forms of Fraud[xvi]

Most Australians are ...

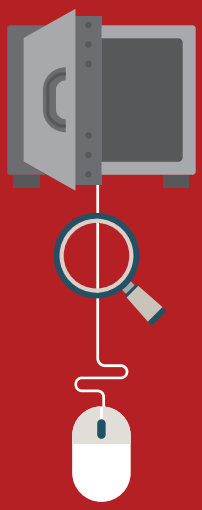
- **69%** regularly checking bank statements for suspicious activity
- **67%** using anti-virus software
- **65%** using Paypal for online payments

But they are not so good at ...

- **36%** using a paper shredder
- **33%** regularly changing online passwords
- **29%** locking their post/letterbox

Figure Ten: How Do Australians Protect Themselves From Fraud? [xvii]

CASE STUDY OF A MULTI-NATIONAL TECHNOLOGY COMPANY



In September 2016, a multinational technology company revealed that data associated with **more than 500 million accounts had been compromised**. The breach, which was estimated to be one of largest reported incidents of its kind, occurred in late 2014. The company also revealed the breach was thought to be **committed by an individual working on behalf of a foreign government**.

By accessing the company's system, the cybercriminals were able to collect account information such as **names, email addresses, telephone numbers, dates of birth,** and **passwords of company users.** In some cases, the hackers may have also stolen security questions and answers, allowing the perpetrators to break in to users' unrelated online accounts.

The company assured users bank account and credit card details had not been stolen, and encouraged people to change their passwords and monitor their accounts for suspicious activity. However, given the time that had lapsed between the breach occurring and the company reporting the incident, many users may still be vulnerable to cybercrime in the future.

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 2016, a survey of 1,000 Australians found:

11%	of Australians report having been a victim of identity theft in the past 12 months, up from 6% in 2015
27%	report they have been a victim of identity theft fraud at some stage in their lives
71%	of Australians are concerned about having their personal information stolen
45%	of people are more concerned about identity theft than they were 12 months ago

If 11% of Australians are falling victim to identity theft and misuse in an average year, this equates to approximately **2.5 million people being affected annually** – and this number is growing.

It is also likely that the number of victims is higher than reported, due to the insidious nature of cybercrime.

In many cases, victims of cybercrime may remain unaware that their personal information has been compromised for months or even years after the fact, as the perpetrator may hold on to their ill-gotten information until they find the right opportunity to use it.

While most Australians are at least somewhat concerned about the safety of their personal information, there is one demographic bucking the trend – millennials.

18-29 year olds are the least concerned about having their personal information stolen. This may be because they are 'digital natives' and feel inherently comfortable online. However, their complacency may put this group at risk, as they take fewer precautions to protect their information – such as using anti-virus software and regularly changing online passwords – than people in other age brackets.

As people become more aware of cybercrime, through media reports and first- or second-hand experiences, a better understanding of the different ways in which crime is perpetrated is fostered among the general population.

In 2016, Australian consumers believed phishing or email scams and card skimming to be the most common forms of fraud (see Figure Nine).

Although social media account hacking is not considered to be one of the more common fraud types, 74% of Australians do not trust social media to protect their personal information.

Despite this mistrust, only **38% of Australians have their accounts on the highest privacy settings** (see Figure Ten). Women are more likely than men to use the highest privacy settings on their social media accounts, which may be because they are more active and share more personal details through these channels.

Australians are generally less worried about sharing their financial details online compared to other personal information. This suggests consumers have faith in banks and financial institutions to protect their details, although **69% of people regularly check their bank statements** for suspicious activity, just to be safe (see Figure Ten).

While knowledge of and concern about cybercrime is growing, many Australians are still dangerously lax in their fraud security measures. This is especially true when it comes to simple actions like regularly **changing online passwords, which only a third of people (33%) actually do** (see Figure Ten).

Individuals living in metropolitan areas have a higher risk of becoming victims of cyber fraud than those who live in rural areas, due to the opportunities metropolitan population density creates for fraudsters.

Of the metropolitan population, people living in high density apartment blocks are some of the most vulnerable. Veda's research shows that residents of apartment blocks with more than 50 units are 40% more likely than average to be victims of identity theft.

This activity can be linked to the **large number of individuals (71%) who leave their letterboxes unlocked**, presenting an easy target for opportunistic identity thieves who can hide in plain sight in high footfall areas like apartment buildings.

From a consumer's perspective, the cost of credit fraud is more than simply lost money. Cybercrime and identity theft can have long-lasting repercussions, including **damage to an individual's credit history, refusal of future credit applications, reputational damage, potential legal costs, mental and emotional strain,** and a **lingering fear** that their details may be used again without their knowledge.

Future Challenges – Cybercrime and Fraud in 2017

In this section, Veda looks ahead to some of the key cybercrime trends and challenges for 2017.

1. **CEO fraud, or cyber-attacks on C-suite executives, will grow.** Techniques such as 'spear phishing', where cybercriminals hook their victims with a malware-infected email that appears to be from a trusted individual or business, will increasingly be used in this kind of attack.

2. **The commoditisation of the tools of cybercrime will also increase.** Cybercriminals will look to build their 'businesses' by swapping and selling stolen information and prewritten malware, or by offering their skills for hire, on the dark web.

3. **State-sponsored cyber espionage will become one of the hottest topics of 2017,** as foreign cybercriminals redouble their efforts to digitally infiltrate government and related agencies – both with and without the knowledge of their own governing bodies.

4. **Ransomware will continue to pose a real threat.** Cybercriminals will focus their efforts on organisations, like legal firms or doctors' surgeries, which hold a goldmine of sensitive personal information but are often less secure than many government or private business databases.

5. **The 'paradox of protection' will come to the fore.** As people become more aware of cybercrime, many will attempt to protect themselves by taking their personal information and professional verification tools offline wherever possible. However, by reverting back to offline methods, many individuals and organisations run the risk of leaving personal details vulnerable to being stolen from low-security storage and migrated online.

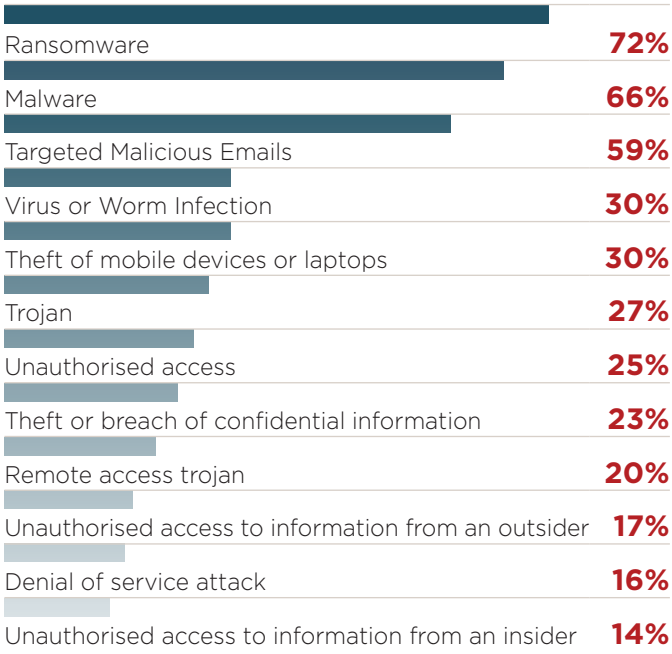
Combatting Cybercrime and Fraud

The key to combatting fraud is to stay on the front foot – there is no such thing as a 'set and forget' cybercrime and fraud prevention system. Fraudsters are constantly on the lookout for new ways to steal information, so businesses and individuals need to be equally tenacious.

PROTECTING BUSINESSES

When setting up or updating cyber security measures, businesses need to have a thorough understanding of where their threats are most likely to come from.

The Australian Government's Cyber Security Survey found that ransomware was the most common type of cyber security incident experienced by Australian businesses in 2015.[xviii]



Multi-layered security systems, combining active and passive layers of protection to break predictability also remain a key tool in combatting cybercrime and fraud. But while cybercrime is often complex, not all measures to protect against it need to be.

Organisations should do away with the idea that protecting against cybercrime and data breach is the exclusive realm of a single department. Keeping all employees well-informed of trends in cybercrime and fraud, and flagging current scams so they don't unwittingly fall victim are easy preventative measures to take.

PROTECTING INDIVIDUALS

All Australians are living in a period of unparalleled digital change. By 2017, 90% of Australians will be online. Two out of three people have social media accounts and, on average, Australians spend the equivalent of one full day a week online.[xix]

Add to that the increasing number of connected devices at our disposal – from phones and watches to refrigerators and even cars – and it becomes clear that the way we live has become inextricably linked with cyberspace.

Unfortunately, the exciting advances in consumer technology has also opened up countless new opportunities for cybercriminals to try and exploit the system.

In many cases, connected devices have less robust built-in security, offering easy access for cybercriminals looking to pilfer personal information. Even devices that collect seemingly trivial data, like a fitness tracker or a smart TV, can be useful to fraudsters.

For consumers, it is up to the individual to remain aware of common scams and learn from past mistakes – either their own or the well-publicised errors of others.

VEDA'S ROLE IN COMBATTING CYBERCRIME AND FRAUD

At Veda, we take our role in combatting fraud and cybercrime very seriously. We are committed to keeping Australians safe against this threat.

Veda's multi-faceted range of products and services spans both the business and consumer markets:

Shared Fraud Database

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

Contributors to the Shared Fraud Database are members of Veda's Fraud Focus Group. Australia's 'big four' banks, international financial institutions, telecommunications providers, motor vehicle financiers and other credit providers including credit unions and asset financiers, all contribute to 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 fraud. Members who are eligible 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 Fraud Focus Group have collective strength.

EACH YEAR, VEDA IDENTIFIES APPROXIMATELY $1 BILLION IN FRAUDULENT CREDIT APPLICATIONS.

Fraudsters can be detected before credit is extended and devices associated with previous fraudulent applications can be red-flagged.

Credit file and personal information alerts

Veda offers credit file alerts so subscribers are notified of certain changes to their credit report. A sample scenario could be when another person uses an individual's personal details to apply for credit fraudulently. An alert would be triggered by the individual attempting to commit fraud in this instance, allowing the subscriber to take immediate action 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 – on internet sources 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 securely stores this information 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 recompense 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.

Identity Verification

Veda developed IDMatrix to provide companies and government agencies with 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 against 25+ independent data sources, including the Government's Document Verification Service. This provides organisations of all sizes with the ability to immediately verify a customer's identity electronically 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 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 whether their prospective tenant has adverse tenancy database listings 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.

For employers, the easiest and most effective way to avoid opening their doors to a fraudster is to carefully screen potential hires, nipping the problem in the bud.

Veda's pre-employment screening business, Verify, offers the full range of pre-employment checks any compliant and concerned employer might require. These checks include identity, domestic and global criminal background checks, qualifications, employment history, credit and licence checks. Enabled by Verify's leading candidate portal, all checks come with electronic ID verification leading to faster and more secure validation.

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 identify people who are not who they claim to be. Veda provides a device intelligence solution which is cloud-based, and offers real-time device identification. It helps to protect businesses against cybercriminals 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 digital identity and location. The system screens transactions against a global database of more than 60 million known fraudulent devices and provides organisations with the insights required to determine whether to proceed, challenge or stop an online transaction.

Veda provides these products and services to the business, government and consumer markets. Veda's fraud and cybercrime team is constantly searching for and developing ways to help all parties protect against the constant and ever-evolving threat of cybercrime.

For more information

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

Email: idmatrix@veda.com.au

Visit:

Consumer Identity Solutions

veda.com.au

Identity Verification Solutions

veda.com.au/idmatrix

Employee Screening

verifycv.com.au

Sources

i. National Plan to Combat Cybercrime p 4. ag.gov.au
ii. Veda Shared Fraud Database 2014/2015
iii. Veda Shared Fraud Database 2015/2016
iv. Veda Shared Fraud Database 2015/16
v. Veda Shared Fraud Database 2015/16
vi. Veda Shared Fraud Database 2015/16
vii. Veda Shared Fraud Database 2015/16
viii. Ponemon Institute 2016 Cost of Data Breach Study: Australia
ix. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094AUEN
x. Australia's Cyber Security Strategy
xi. https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf
xii. 2015 Cyber Security Survey: Major Australian Businesses
xiii. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094AUEN
xiv. Ponemon Institute 2016 Cost of Data Breach Study: Australia
xv. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094AUEN
xvi. Ponemon Institute 2016 Cost of Data Breach Study: Australia
xvii. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094AUEN
xviii. Australian Payments Fraud: Details and Data. Australian Payments Clearing Association 2016.
xix. http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf
xx. Australian Payments Fraud: Details and Data. Australian Payments Clearing Association 2016 p 26.
xxi. http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf
xxii. Australian Payments Fraud: Details and Data. Australian Payments Clearing Association 2016 p 3.
xxiii. http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf
xxiv. Veda Commissioned Survey. The Leading Edge: Survey of 1000 Australian Adults, September 2016
xxv. Veda Commissioned Survey. The Leading Edge: Survey of 1000 Australian Adults, September 2016
xxvi. 2015 Cyber Security Survey: Major Australian Businesses p 23.
xxvii. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094AUEN
xxviii. Australia's Cyber Security Strategy p 14.
xxix. https://cybersecuritystrategy.dpmc.gov.au/assets/pdfs/dpmc-cyber-strategy.pdf

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**