Australian Government
Australian Institute of Criminology

AIC reports
Research Report 15

National Identity Security Strategy

Estimating the cost to Australian businesses of identity crime and misuse

Russell G Smith

ISSN (Online) 2206-7280

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: aic.gov.au

Please note: Minor revisions are occasionally made to publications after release. The online versions available on the AIC website will always include any revisions.

All publications in the Research Report series are subject to peer review–either through a double-blind peer review process, or through stakeholder peer review. This report was subject to stakeholder peer review.

Disclaimer: This research report does not necessarily reflect the policy position of the Australian Government.

General editor: Dr Rick Brown, Deputy Director, Australian Institute of Criminology

Edited and typeset by the Australian Institute of Criminology

A full list of publications in the AIC Reports series can be found on the Australian Institute of Criminology website at **aic.gov.au**

Contents

Figures

Tables

Acknowledgements

This research was commissioned and funded by the Department of Home Affairs. Research assistance was provided by Rebecca Savage and Catherine Emami, formerly Research Officers at the Australian Institute of Criminology, and Marissa Hood, Research Librarian at the Institute. Penny Jorna, Research Analyst at the Institute, also provided feedback on an earlier version. The incidence and cost estimates were reviewed by a panel of 12 government and business specialists in identity crime and misuse. The opinions expressed are those of the author alone.

Acronyms and abbreviations

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ASIC	Australian Securities and Investments Commission
AusPayNet	Australian Payments Network
EFT	electronic funds transfer
GDP	gross domestic product
IVA	industry value-add

Executive summary

Misuse of personal information affects not only individual consumers, who may have their identity stolen or banking details misused when making online transactions, but also business enterprises. Risks for businesses of all sizes include:

- email phishing attacks;
- misappropriation of commercial property, including client lists, logos and names;
- invoicing and funds transfer fraud;
- frauds involving the misuse of business information;
- misrepresentation of instructions of chief executive officers concerning funds transfers; and
- various business opportunity and investment scams.

In Australia, there are over two million businesses, most of which are micro or small businesses that often do not have the capacity to lose assets to identity misuse and frauds of this nature, or the resources to deal with the consequences of frauds. On the most serious occasions, identity crime losses will lead to the total failure of the affected business.

This study examined the economic scale of the problem of identity crime and misuse targeting businesses in Australia. Although little research has been conducted to assess the scale and cost of this type of crime, this study provides estimates of the direct and indirect costs borne by affected businesses.

Although the baseline data are not sufficient to support precise estimates, it is estimated that, in 2017, the financial impact of identity crime on business in Australia was between $1.4b and $2.0b.

Further research is needed to gather more data to improve the accuracy of these estimates and to understand the full economic and commercial consequences of identity crime for the Australian business sector.

Introduction

This report estimates the economic cost of identity crime and misuse to the Australian business sector. Prior research has quantified the general extent and cost of identity crime throughout Australia. For 2015–16, direct costs were estimated to be $2.1b, and the additional indirect costs of preventing and responding to crimes of this nature were estimated to be $596m. The total economic impact was, accordingly, $2.65b for the 2015–16 financial year (Jorna & Smith 2018). This includes direct and indirect costs to government, the private sector and individuals.

Considerable research has been undertaken to quantify the extent and cost of identity crime affecting individuals, as much of this type of crime targets people in the community, particularly those who use the internet for online shopping (ABS 2012; ACCC 2018; ACCC 2017b). Less attention has been given to identity crime that affects businesses, although research in this area is gaining strength in Europe (Anderson et al. 2012; Centre for Counter Fraud Studies 2017; National Audit Office 2017; Paoli et al. 2017). There is now an appreciation that studies using small sample sizes and a limited focus on direct out-of-pocket losses misinterpret the scale of the problem. Much more sophistication is needed to define the crime categories involved, to understand the range of losses that can be measured, and to more precisely quantify indirect and intangible losses for enterprises.

Businesses can experience identity crime victimisation in various ways, including:

- responding to unsolicited mass-marketed scam invitations;
- having their corporate identity stolen or misused by criminals seeking to defraud their customers or others in the community;
- suffering misappropriation of commercial property, including client lists, logos and names;
- invoicing and funds transfer fraud;
- fraud relating to payment cards and credit facilities;
- frauds involving the misrepresentation or misuse of personal information belonging to Chief Executive Officers; and
- business opportunity and investment scams.

In the United States, the National Association of Secretaries of State (2012) published a comprehensive white paper on business identity theft, citing 'a wide range of scenarios involving the fraudulent or unauthorised use of a company's identity' (NASS 2012: 5). In many respects, business operations are subject to similar risks of identity crime as consumers, although arguably their exposure is greater owing to the assets they control, their reputational capital and their greater online presence.

Although a number of business crime victimisation surveys have been conducted (eg Burrows et al. 1998; Walker 1994), few examined economic crimes, instead focusing on property loss through burglary, shoplifting, damage caused by vandalism, employee fraud, and violent crimes against staff. Some business victimisation surveys examined external fraud risks, particularly involving large corporations, but these have rarely considered the specific problem of fraud and dishonesty involving misuse of identifying corporate information. The exception is the financial services sector, which regularly quantifies payment transaction fraud, most of which entails theft of account information or other banking credentials—in other words, identity crime and misuse (AusPayNet 2017).

A number of studies have provided estimates of the cost and impact of cybercrime (see the review and evaluation by Anderson et al. 2013). A review by Paoli et al. (2017) shows that, although these studies have included identity crime and misuse to varying extents, many suffer from a variety of methodological limitations. In particular:

> …the studies produced by consulting and security companies are often not explicit about their conceptualization of cybercrime, cost and impact, and their methods of data collection and assessment. They have also been criticized for overestimating—and even artificially inflating—both the incidence as [sic] the economic impact of cyber incidents. (Paoli et al. 2017: 11).

It is also important to consider the numbers and types of respondents to business victimisation surveys. Often, consultancy research is based on small sample sizes and limited to large corporations—usually derived from the client base of the consultancy firm in question. Findings from such studies should, of necessity, be restricted to organisations of a similar nature, not extrapolated more widely; for example, compared with large-scale enterprises, small enterprises often experience costs and impacts of a substantially different nature. Simply grossing up findings from small-scale surveys of large corporations and applying them to the entire business sector produces findings that are unjustifiable and methodologically problematic.

Finally, it is important to consider the financial impact on the victims of identity crime. On the one hand, identity crimes can directly affect businesses, especially where perpetrators—either from within organisations or externally—commit fraud or other crimes that entail misuse of business identity information, or manipulate an individual's personal information to steal business assets. On the other hand, businesses can be indirectly affected by suffering losses and incurring costs when they compensate their customers who are victims of identity crime that has occurred through the use of their business.

The clearest example of this involves financial institutions that agree to refund customers for losses from fraudulent banking transactions, such as automatic teller machine (ATM) skimming or phishing, where the customer is found to be blameless. ATM skimming offenders use illegal card readers and micro-cameras to record account details and personal identification numbers (PINs) at ATMs, allowing them to make unauthorised withdrawals from that ATM. Phishing offenders obtain personal information via illegal websites that trick users into disclosing information that can then be used fraudulently.

In many cases where consumers have been the victims of identity crime, the financial loss will be shifted from the financial institution to the retail merchant as a chargeback. As a result, much of the cost of identity crime that is initially experienced by individuals is, in fact, ultimately borne by either financial institutions or retail businesses. In some cases, the actual losses to businesses may be recovered from insurers. In estimating the overall cost of identity crime to the business sector, this shifting of loss from consumers to organisations needs to be counted in the final assessment.

Methods and scope

This study brings together the limited existing information on identity crime and misuse affecting the Australian business sector and provides estimates of the current extent of the problem and the scale of its direct and indirect costs. The report does not provide definitive estimates; accordingly, it should be seen as a platform for developing further research and undertaking more thorough and precise analysis. It shows the knowledge gaps that exist and identifies avenues for further empirical study.

This report presents an extensive review of more than 30 studies and official datasets on business victimisation that are relevant to Australia. The key facts from the 10 most influential sources in Australia are presented in the appendix. From this review, it is apparent that few, if any, studies quantified the economic and other impacts of identity crime and misuse on the Australian business sector. Instead, the collection provides a variable set of indicators of the cost of some elements of the problem, often combined with other types of business illegality that are unable to be disaggregated. Identification of the costs and impacts that relate solely to identity crime and misuse is the most difficult aspect of the topic.

The preferred approach, which is beyond the resources of most public and private sector entities, is to commission new data collection exercises that could yield precise information on the extent of the problem in all its many forms. This would, ideally, combine a multi-method study employing survey research coupled with analysis of business records and interviews with accounting and auditing personnel in the relevant sectors.

In order to delimit the scope of the present inquiry, and to clarify what was being measured, a number of terms and concepts are first defined. The following definitions align with those used in the report *Identity crime and misuse in Australia 2017* (Jorna & Smith 2018). However, care must be taken when comparing data from other studies that might have used different definitions and data collection categories.

Business identity crime and misuse

Identity crime is a generic term used to describe activities and offences in which a perpetrator uses a fabricated identity, a manipulated identity or a stolen or assumed identity to facilitate the commission of crime (Australasian Centre for Policing Research 2006).

Identity misuse is a more general concept that involves use of personal information without authorisation that might not necessarily entail breach of a criminal law.

Business identity crime pertains to business entities. Businesses are not subject to all types of identity crime and misuse (the most prevalent involve online payment system fraud; phishing and misuse of business identities to facilitate other forms of transaction fraud, such as false invoicing; and other forms of deception relating to contractual obligations, including payment card fraud). Some categories of business fraud and crime do not ordinarily entail misuse of identity. These include various forms of ransomware attacks in which threats to encrypt, or refusal to decrypt, data are made unless payments are made to criminal enterprises. Although the identity of the offender in such attacks is disguised through various means, business information is not stolen and payments are made to real criminal enterprises.

The Australian Competition and Consumer Commissioner (ACCC) in *Targeting scams: Report of the ACCC on scams activity 2017* (2017b: 22) identified the following types of business scams.

- *Business email compromise scams* occur when a scammer obtains access to business email addresses and customer lists, through either a virus or a successful phishing attack. These scams come in various forms. Typically, the scammer pretends to be from the targeted business and sends an email (purportedly from upper management) to its customers, advising of new payment arrangements and requesting an immediate funds transfer to a new account. In other cases, the scammer will impersonate the chief executive officer of a targeted business and send an internal email to the accounts department redirecting payment of an invoice to a fraudster. These emails look legitimate and appear to come from the correct email address.
- *Ransomware* is a type of virus that infects computer systems and encrypts the device to prevent user access until payment, in the form of bitcoins or funds transfer, is made to unlock it. These emails ask the recipient to follow a link or open an attachment, causing malicious software to be downloaded. Most types of ransomware attack do not involve misuse of identity; the perpetrator attacks a business entity not by using a fabricated identity but with encryption software such as an onion router, which makes it difficult to identify the perpetrator. Ransomware is, therefore, a 'pure' form of cybercrime in which data are damaged through the use of malware; it does not rely on social engineering or other forms of dishonesty to deceive the business entity.
- *False billing scams* generally request businesses to pay false invoices for advertising, domain name renewals or office supplies. These scams take advantage of the fact that the person handling the administrative duties for the business may not know whether the promotional advertising or office supplies have in fact been requested and might make the payment without first verifying the invoice.
- *Investment scams* target many types of investments, including sports investments, stockbrokers, superannuation schemes and managed funds. They are often promoted as business opportunities and promise inflated returns.

Fraud against a business entity can involve misuse of business identity information, principally by:

- businesses falling victim to generic consumer scams by perpetrators using a false identity;
- fabrication of financial transactions, with the use of false accounts or customer information;
- misappropriation and misuse of the business identity, such as its name, logo, website and account details, often involving unauthorised access to networks; and
- phishing involving business identities and online resources that seek to obtain information and funds from victims.

In the ACCC's (2018) report *Targeting scams*, an example was given of a small business email compromise scam reported to the ACCC's Scamwatch website in 2017 (Box 1).

Box 1: Case study, small business email compromise scam

A scammer hacked into our boss's email account in May 2017. The scammer studied how he communicated to me because I am in charge of the accounts mailbox which is used for money transfer requests.

In July, when our boss was overseas, the scammer sent an email from my boss's email address to our accounts mailbox asking for a transfer of $67,000 to an external account. I thought it was a legitimate instruction from the boss so I made the transfer. When the boss returned later in the month, it was only then that we realised that it was a fraud and that our boss had not made that request.

We could not find the email I received in our boss's email account. The scammer must have deleted it to cover his tracks. We have reported the incident to the bank and police and we are awaiting their investigation but we fear it is too late to get the money back.

Source: ACCC 2018: 23

Estimating the extent of business identity crime

A variety of approaches can be used to estimate business losses arising from misuse of personal and corporate information in business environments. For some of these approaches, it is necessary to estimate the proportion of relevant reported crime that could involve misuse of business identity or other forms of identity misuse in connection with the commission of the criminal conduct against business organisations. This estimation process relies on previous administrative and self-reported victimisation data in connection with specific subcategories of identity crime. Ratings can then be applied to the nature of the criminal typology or methodology employed in the conduct. For some crime types, the methods are well-known and relatively uniform; in others, the techniques are novel and variable, particularly with respect to misuse of identity.

Percentages can be estimated for each business crime category. However, given the data currently available, this is often a subjective indication of its extent—it is not based on precise empirical data. Estimates for some forms of identify crime will be far more informed by objective evidence than others. To reflect this, the following ratings can be assigned to indicate the estimate's degree of certainty:

1. low certainty;
2. medium certainty; and
3. high certainty.

The rankings above follow those used by the National Fraud Authority (2013: 6) to estimate the cost of fraud in the United Kingdom. A three-tier confidence rating (bronze, silver and gold) has also been used in the more recent Annual Fraud Indicator developed by the Centre for Counter Fraud Studies in the UK (2016, 2017).

The ratings used in this study have been peer-reviewed by 12 identity crime specialists from government, business and academic sectors in Australia and overseas. The following estimates were subject to peer review:

- proportion of Scamwatch reports by businesses that entail identity crime (Table 4);
- multiplier used to inflate Australian Cybercrime Online Reporting Network (ACORN) reports to account for unquantified and unreported matters (Table 5);
- proportion of losses reported in the *Identity crime and misuse in Australia 2017* report that involved businesses (Table 7);
- proportion of individual victims of personal fraud who were victimised in respect of their small business operations;
- proportion of prevention and response costs reported in the Identify Crime and Misuse survey that involved business operations;
- proportion of prevention and response costs reported in the *Identity crime and misuse in Australia 2017* report that involved identity crime and misuse;
- proportion of reported fraud that involved identity crime and misuse; and
- proportion of industry value-add (IVA) for each industry division that involved identity crime and misuse (Table 8).

It should be emphasised that the 12 peer reviewers were not always able to comment on some of these estimates, because either the task was beyond their expertise or baseline data simply did not exist. Accordingly, the final estimates given below cannot be said to be based on definitive empirical data; they are simply based on the best estimates provided by the author, confirmed or varied by those reviewers who were comfortable with offering an opinion. Where reviewers differed on any individual estimated percentage, these were averaged across all the estimates given.

Businesses and sectors

This study relates to all private sector business enterprises, including incorporated entities, incorporated associations, partnerships, sole trading registered businesses and trusts, as well as public sector corporations. Enterprises of all sizes were included.

In terms of vulnerabilities to identity crime and misuse, sole traders are most likely to be victimised in similar ways to individual consumers, although business-oriented scams are more likely to be problematic than personal violations such as romance fraud or lottery fraud. The Office of the New South Wales Small Business Commissioner (2017) estimated that 60 percent of cybersecurity events impact on small and medium enterprises, costing them an average of $50,000 per incident. The ACCC's (2018) report *Targeting scams* provided a breakdown of scams reported to Scamwatch by business size, presented in Table 1.

Table 1: Scamwatch reports in 2017 by size of reporting business and loss

Employees	Reported loss	% of total losses	Reports (n)	% of reports
Micro (0–4 staff)	$740,132	16.0	1,505	27.8
Small (5–19 staff)	$2,249,836	48.8	1,430	26.4
Medium (20–199 staff)	$812,040	17.6	797	14.7
Large (>200 staff)	$503,138	10.9	350	6.5
Unknown	$308,508	6.7	1,334	24.6
Total	$4,613,654	100.0	5,416	100.0

Source: Adapted from ACCC 2018: Table 12

Table 2 presents the latest Australian Bureau of Statistics (ABS) data on the number of businesses in Australia (ABS 2017b).

Table 2: Number of Australian businesses by sector on 30 June 2016

Sector	Number
Companies	804,186
Sole proprietors	561,033
Partnerships	276,303
Trusts	529,606
Public sector corporations	416
All organisational types	2,171,544

Source: ABS 2017b: Table 10

Table 3 presents ABS data on Australian businesses by employment size (ABS 2017b).

Table 3: Number of Australian businesses by employment size on 30 June 2016	
Employment size	**Number**
Non-employing	1,318,579
1–4	599,408
5–19	198,721
20–199	51,024
>200	3,812
Total employing	852,965
Total	2,171,544

Source: ABS 2017b: Table 13

Geographical location

Identity crime can extend across jurisdictional borders. This is particularly so for types of identity crime that involve electronic funds transfer (EFT), such as by payment cards or Bitcoin credits. Therefore, it is important to demarcate the geographical boundaries of this research.

This study relates to identity crimes that target Australian registered businesses, regardless of where the perpetrator is located, subject to Australian courts having criminal jurisdiction.

Cost elements

The elements included in the costs of identity crime and misuse are:

- direct losses actually incurred as a result of victimisation, taking into account any funds recovered through insurance, refunds or compensation (net out-of-pocket losses); and
- indirect losses, including the costs of preventing and responding to identity crime, intangible impacts and lost output through lost opportunity costs and disruption to business.

In addition, as noted above, some businesses experience losses through compensating their customers who have experienced identity crimes, or repaying financial institutions who have reversed illegal customer transactions.

For those cost elements unable to be quantified precisely, estimates are given of the likely global costs involved in some categories.

Reference period

An attempt has been made to rely on data relating to the financial year 2016–17. Where data relate to other periods, the findings have been inflated to reflect what would have been experienced in 2016¬–17. This was done using the Reserve Bank of Australia's online inflation calculator, which uses its consumer price index inflation rates (RBA 2018). For example, the calculator shows that $100 in 2013–14 was equivalent to $104.88 in 2016–17. Inflation rates were applied at the last stage of the conversion process. This method of inflation has been used only where it is appropriate to vary data from before 2016–17.

Exclusions

Excluded are losses caused through scams and malware, such as ransomware, that do not entail misuse of identity, in which demands are made for money in exchange for damaged systems to be reinstated or for data to be decrypted. In these cases, there is no attempt made to disguise the identity of the perpetrator or other actors.

Existing Australian data

Payment system fraud in 2016 ($540m)

The Australian Payments Network (AusPayNet) publishes annual payment fraud statistics for incidents reported by Australia's financial institutions and major card schemes. The latest data relate to the 2016 calendar year (AusPayNet 2017). Because payment system fraud entails perpetrators using another individual's payment card or account information for financial gain, it can be assumed that almost all such instances entail identity crime or misuse.

In any year, the number of instances in which customers are found to have contributed to the loss arising from an unauthorised transaction under the ePayments Code (ASIC 2016) is relatively minimal. In 2003–04, for example, of the 18,802 complaints involving unauthorised EFT transactions in which the device and/or access method was lost or stolen or security was breached, the customer was found to be liable in 42 percent of matters (7,897). Taken as a percentage of the total 2,529,550,988 EFT transactions in 2003–04, customers were liable in only 0.0003 percent of transactions. For present purposes, these may be disregarded (ASIC 2005: 24). More recent statistics on the number of customers found to have contributed to losses arising from an unauthorised transaction under the ePayments Code are not publicly available (S Nanda [ASIC], personal communication 13 September 2017).

Because cardholders are required to notify card issuers of misuse or fraud, it can be assumed that the vast majority of matters come to the attention of AusPayNet, and that unreported losses could be discounted from the cost of identity crime and misuse involving payment systems. Against this argument is the risk that some cardholders who are complicit in the fraud, or who have acted negligently, might be unwilling to report their loss to their card issuer. The above data show that only a very small number would appear to have been responsible in some way for the fraud that occurred.

In 2016, AusPayNet (2017) reported, 2,840,650 transactions worth $540,200,415 were fraudulent, representing 0.03 percent of the number of all transactions and 0.029 percent of the value of all transactions. This forms the bulk of identity crime and misuse relating to the financial services sector. Other types of identity crime within financial institutions, such as internal fraud involving misuse of identity by staff, are included in sections below.

ACCC identity crime scams targeting business ($3.6m)

The ACCC report on scam activity for 2017 included data on reports of scams targeting Australian businesses (ACCC 2018). These totalled 5,432 in 2017, with 427 Australian businesses losing a total of $4,669,409. This represents 3.4 percent of the total number of 161,528 scam reports made to Scamwatch, or 5.1 percent of the total losses of $90,928,622. Of the total losses suffered by businesses, $4.7m, micro and small businesses lost approximately $3m (64.9% of all business scam losses). The average loss was $10,935.

Not all of these reports entailed misuse of identity. Table 4 shows the subcategories of business scams and estimates of the proportion that might have involved misuse of identity in some way. The estimates were assessed by 12 external experts during peer review. Percentages and ratings of panel members who were able to provide these estimates were averaged.

Misuse of identity in connection with business scams could have occurred where:

- the perpetrator pretended to be another person or business;
- bank account information belonging to another was used without authority;
- the victim organisation's identity (such as their logo, name or URL) was taken over by the perpetrator; and
- any other case in which identification information had been misused.

Table 4 also provides an estimate of the reported losses that might have involved misuse of identity, based on the average percentages estimated. On average, 38.8 percent of reported business scam losses might have involved misuse of identity. The category of business scams that most involved misuse of identity (identify theft involving spam or phishing) accounted for 376 reports, only six of which identified a loss. These six reports, however, had total losses of $137,775—the fourth highest loss category. Although the Scamwatch website did not list a specific category for business email compromise scams, ACCC's analysis (2018) revealed more than $1.2m in reported losses for this scam type.

Table 4: Scamwatch reports by businesses 2016 and identity crime estimates

Scam category	Reported loss ($)	Reports (n)	Reports with loss (n)	Identity crime (%)[a]	Identity crime loss ($)
False billing	1,470,148	1,323	106	59 (2)	867,387
Hacking	581,537	177	22	57 (2)	331,476
Other business, employment and investment scams	1,659,465	658	46	10 (2)	165,947
Identity theft involving spam or phishing	137,775	376	6	100 (3)	137,775
Other buying and selling scams	407,381	592	89	25 (1)	101,845
Other upfront payment and advanced fee frauds	118,316	412	25	76 (3)	89,920

Table 4: Scamwatch reports by businesses 2016 and identity crime estimates

Scam category	Reported loss ($)	Reports (n)	Reports with loss (n)	Identity crime (%)[a]	Identity crime loss ($)
Remote access scams	55,875	73	7	55 (3)	30,731
Phishing	29,140	654	4	86 (3)	25,060
Fake trader websites	22,729	149	41	90 (3)	20,456
Fake charity scams	21,168	105	23	89 (3)	18,840
Classified scams	53,201	102	23	10 (1)	5,320
Overpayment scams	35,503	107	7	12 (1)	4,260
Nigerian scams	4,820	40	1	80 (3)	3,856
Computer prediction software and sports investment schemes	6,050	2	1	41 (2)	2,481
Ransomware and malware	38,754	124	7	5 (2)	1,938
Threats to life, arrest or other	2,090	135	1	59 (2)	1,233
Investment schemes	9,600	22	3	11 (3)	1,056
Reclaim scams	10,000	104	1	10 (1)	1,000
Mobile premium services	1,738	27	13	9 (1)	156
Health and medical products	4,119	43	1	3 (2)	124
Unexpected prize and lottery scams	0	58	0	70 (3)	0
Inheritance scams	0	55	0	66 (3)	0
Job and employment	0	49	0	10 (1)	0
Travel prize scams	0	34	0	77 (3)	0
Dating and romance	0	7	0	81 (2)	0
Pyramid schemes	0	2	0	21 (1)	0
Scratchie scams	0	1	0	10 (1)	0
Psychic and clairvoyant	0	1	0	56 (2)	0
Total	**4,669,409**	**5,432**	**427**		**1,810,861**
Mean			**7.9**	**38.8**	**4,249**

a: Numbers in parentheses are confidence ratings: 3=high certainty, 2=medium certainty, 1=low certainty
Source: ACCC 2018: Appendix 3

Of the reports made, only 7.9 percent identified a loss, either because there was no financial loss or a financial loss had not yet been identified or could not be quantified. In addition, the peer review panel examining the data estimated that business cybercrime reporting rates to official government agencies were between nine and 58 percent. Identity theft was estimated to have the highest reporting rate of 58 percent, compared with 50 percent for online buying and selling fraud, 43 percent for scams and fraud generally, 20 percent for computer system attacks and viruses, 17 percent for spam and phishing, and nine percent for online bullying, sexting, harassment and stalking.

If the estimate in Table 4 of business identity crime losses of $1,810,861 is inflated by two to account for unquantified and unreported incidents, this would entail a total potential loss of $3,621,722, including both reported and unreported incidents. It should be noted that this amount includes some losses included in the fraudulent transactions recorded by AusPayNet (2017; see *Payment system fraud in 2016*, above).

ACORN business identity cybercrimes 2016–17 ($130.2m)

Online scam reports made to ACORN in 2016 totalled 45,068, costing $204,705,578. Only 38 percent of reports indicated a loss amount, and those losses reported were the individual's own assessment of their loss. Of the total reports made, 5,443 involved online identity theft. Of these, 2,441 reports indicated loss amounts totalling $23,450,818.

ACCC (2018) analysis of more recent ACORN data for 2017 found that 7,645 reports involved online identity theft. In 3,927 reports a loss amount was provided, with losses totalling $43,769,762. These reports came from all victims, not only businesses.

For the financial year 2016–17, the victim had an 'organisation name' in 4,071 reports, and so it could be assumed that these were indicative of business victims of online cyber attacks. Data provided by ACIC (2017) disclosed seven categories of such cyber attacks:

- attacks on a computer system or virus;
- cyberbullying, sexting, online harassment or stalking;
- online purchase or sales;
- online identity theft;
- online scams or fraud;
- spam or phishing; and
- other and unidentified reports.

Table 5 shows the total dollar losses associated with the categories listed above, with the number of reports involved that disclosed a dollar loss, a zero loss or a non-financial loss. For the reports with an identified dollar loss, Table 4 also shows the losses reported where 'misuse of identification information' had been recorded. Although the data are somewhat unclear as to which reports included an element of identity crime and misuse, the reports that fell into the 'misuse of identification information' subcategory would clearly involve identity crime—these reports alone involved monetary losses of $43,391,598, which was 20 percent of the total ACORN business losses for 2016–17 of $218,176,101.

Table 5: ACORN business victimisation loss data

Category	Report (n)	Zero loss (n)	Non-dollar loss (n)	Dollar loss (n)	Estimated total loss ($)	Identify information loss[a] (n)	Identity information loss[a] ($)
Computer system attack or virus	545	155	115	275	61,147,333	16	3,071,259
Bullying, sexting, harassment, stalking	123	57	49	17	5,029,060	5	1,012,910
Buying and selling online	394	23	136	235	1,152,398	1	1,700
Identity theft	295	155	0	140	22,693,495	26	2,162,561
Scam or fraud	1,809	663	442	704	62,115,131	22	10,004,180
Spam or phishing	333	284	0	49	30,476,399	1	27,000,000
Other	572	235	134	203	35,562,285	10	138,988
Total	**4,071**	**1,572**	**876**	**1,623**	**218,176,101**	**81**	**43,391,598**

a: The dollar loss reported for cases identified as having identification information misused
Source: ACCC 2018

In a similar manner to the reports made to Scamwatch (ACCC 2018), it could be possible to inflate the ACORN business losses to account for unquantified and unreported cases. Of the reports made, only 40 percent identified a dollar loss amount, because either there was no financial loss or a financial loss was not yet identified or could not be quantified. Assuming that only 56 percent of frauds are reported (ACCC 2017b: 21) and taking into account the unquantified cases, the ACORN business identity crime losses of $43,391,598 could be inflated by three to account for unquantified and unreported incidents, to achieve a total potential estimated loss of $130.2m.

These reports of financial loss should, however, be treated with caution. They are the sums that businesses indicated were associated with the attack, without further verification or explanation. The reports have not been tested in court; they must be considered only allegations of cybercrime. Reported losses could also include reporters' estimates of indirect losses—sometimes involving many millions of dollars. On other occasions, monetary losses could not be quantified or were restricted to direct losses. Finally, these loss estimates give no indication of matters that were undetected or not reported to ACORN. As a result, these figures represent only a general indication of how much businesses in Australia might have lost from cyber attacks involving misuse of identity.

In addition, there is considerable overlap between the estimated identity crime losses identified in ACORN reports and those recorded in Scamwatch data (ACCC 2018) and AusPayNet (2017) data. It is not possible to determine the extent of such overlap using the data available.

Australian Cyber Security Centre research

As part of the Australian Government's Cyber Security Strategy (Department of the Prime Minister and Cabinet 2016), the Australian Cyber Security Centre (ACSC) provides information on threats to business arising from online transactions, including identity crime.

The Computer Emergency Response Team (CERT) Australia is one of the ACSC's partner agencies. CERT Australia is the national organisation that works with major Australian businesses to provide cybersecurity advice and support for critical infrastructure and other systems of national interest. In 2015–16, CERT Australia responded to 14,804 cybersecurity incidents affecting Australian businesses (ACSC 2016).

In 2015 the ACSC published the results of its cybersecurity survey of 149 respondents from more than 12 industry sectors. The greatest representation was from the defence industry sector (18%), followed by the energy sector (17%), and the banking and finance sector (11%). It was found that 50 percent of respondents had experienced at least one cyber incident in the past year, with 8 percent of respondents unsure if they had (or had not) experienced a cyber incident. Many of the respondents (43 percent) did not report incidents to anyone (ACSC 2015).

Of the cyber incidents reported, 23 percent involved theft or breaches of confidential information, 14 percent unauthorised access to information from an insider, and 18 percent unauthorised access to information from an outsider. These categories would most likely have involved identity misuse, although no information was collected on identity crime and misuse specifically, and no data were collected on the cost or impact of incidents.

The ACSC (2016: 36) indicated the types of direct and indirect costs associated with security incidents but did not provide dollar values. The following types of costs were identified in the report:

- resources to investigate the extent of the intrusion, understand the harm, and immediately remediate the effects of the intrusion (eg by cybersecurity specialists);
- reactive implementation strategies to mitigate further intrusions. It is more expensive to respond to an incident than to implement proactive strategies, as time frames are more compressed;
- lost productivity and income, and the costs of diverting staff and resources from other business to deal with a compromise;
- loss of revenue associated with the theft of information, such as intellectual property or information about Australia's negotiating position;

- broader costs to the Australian economy where information is stolen from networks (eg personal information used to conduct fraud);
- reputational costs, including negative news and social media exposure, and loss of customer trust (eg where online service is disrupted);
- costs associated with breaching privacy legislation, or remediating data breaches of financial information;
- legal costs where third parties sue for negligence or breach of contract; and
- loss of trust by partners (government or industry), which in turn harms domestic and international relationships critical to the organisation.

Small business scam survey 2013

One of the few national surveys in Australia specifically designed to examine scams against small businesses was conducted by Weber and Geneste (2012) (see also Schaper & Weber 2012). With recruitment assistance by 24 business associations, 291 businesses responded to the survey, with the highest number of respondents coming from retail trade (39), health care and social assistance (19), professional, scientific and technical services (18) and other services (29). Useable responses came from 192 businesses, with annual turnovers ranging from $10,000 to $20m per annum. The most frequently reported turnover category was $1m to $2.5m.

In terms of victimisation, 139 of the 192 respondents (72%) reported receiving a scam invitation in the preceding year. Of the 192 respondents, 23 (12%) reported an actual financial loss, with an average loss amount of $1,258 and a maximum loss of $10,000. Total losses were not reported.

Assuming that 12 percent of small businesses have suffered a financial loss from scams, that there are 2.1m small businesses with fewer than 20 employees or no employees (as shown in Table 2), and that the mean loss of scams is $1,258, this would result in an estimated $318.7m total loss for all small businesses in Australia. However, this fails to account for different victimisation rates across small business sectors, as well as the small sample size in the 2013 survey. Further, Weber and Geneste's (2012) survey does not permit identification of which scams involved identity crime and misuse.

Overseas estimates

Action Fraud (UK)

In the UK, the online fraud reporting portals Action Fraud and Get Safe Online reported £45,150,532 lost by businesses in London to online crime, involving 37,070 crimes reported from 31 March 2015 to 31 March 2016—excluding undetected and unreported cases (City of London Police 2016). Fraud specifically involving misuse of identity included so-called 'mandate fraud' in which:

> …a fraudster gets victims to change a direct debit or standing order by pretending to be an organisation a victim makes regular payments to, for example a business supplier or subscription service. (n.p.)

This accounted for losses of £1,194,287 in 2015–16. Misuse of payment cards involved £14,482,052. Although the identity crime elements were not specified, both retail fraud and insurance fraud can entail misuse of business information—both these fraud types were found to be costly. Both payment transaction fraud and advance fee fraud against businesses declined between 2015 and 2016 (City of London Police 2016). If the reported losses of £15.7m are inflated by two to account for undetected and unreported matters (ACCC 2017b: 21), the total is £31.4m.

Fraud indicators (UK)

Between 2010 and 2013, the National Fraud Authority in the UK published four fraud loss measurement exercises to estimate the scale and nature of the problem of fraud and to raise awareness. These estimates covered both detected and hidden fraud against all UK victims, including the public, private and third sectors as well as individuals. In the private sector, £21.2b was estimated to be lost to fraud in 2011–12, as shown in Table 6.

Table 6: National Fraud Authority estimate of private sector fraud losses 2011–12 (£m and % turnover)

Business victim category	Identified	Hidden	Total	Confidence
Small enterprises (1–49 employees)	4,600 (0.53%)	3,100 (0.60%)	7,700	Good
Medium enterprises (50–249 employees)	44 (0.01%)	1,400 (0.32%)	1,500	Good
Large enterprises (>250 employees)	555 (0.03%)	6,100 (0.38%)	6,600	Good
Financial and insurance activities	515	4,900	5,400	Poor

Source: National Fraud Authority 2013: 17

The National Fraud Authority (NFA 2013) estimated that individuals lost £3.3b to identity fraud in 2012–13, based on the findings of a nationally representative survey of 4,213 UK adults conducted in December 2012.

A survey was also conducted of 500 small, medium and large businesses, excluding 'sole traders' and the 'financial and insurance activities sector'. The study found:

> …of those victims that actually suffered financial loss (that is excluding those that were able to recover their loss or did not know about the loss) an estimated £5.2b may have been lost to fraud during the last financial year. This equates to 0.18 per cent of UK business turnover when extrapolated to all businesses (excluding those from the financial and insurance activities sector, and sole traders). (NFA 2013: 17)

Respondents also indicated that 0.36 percent of their turnover was lost to undetected fraud in 2012–13, while 0.54 percent of turnover was lost to detected fraud in 2011–12.

The NFA (2013: 30) also estimated that, in 2012–13, identity fraud accounted for '14.1 percent of charity fraud victims and 18 percent of private sector fraud victims'.

In the absence of more recent government fraud estimates in the UK, a number of other attempts have been made to quantify fraud loss. In 2015, Financial Fraud Action UK (2016) reported that fraud relating to online and phone banking, debit and credit cards, and cheques was £755m, a 26 percent increase on 2014. In 2016, the British Retail Consortium (2017) crime survey estimated that 53 percent of reported fraud in the retail industry was 'cyber-enabled', equivalent to losses of £100m.

In 2016, Experian, PKF Littlejohn and the University of Portsmouth's Centre for Counter Fraud Studies (CCFS 2016) created a partnership to gauge, analyse and quantify the true scale of fraud in the UK. Private sector fraud losses were estimated to amount to £143.6b, with charities and charitable trusts losing a further £1.9b. These estimates were based on an estimated proportion of business expenditure lost to fraud, rather than on a percentage of gross domestic product (GDP). Identity-related fraud losses were not disaggregated, although phishing was estimated to cost £280m in 2015.

In 2017, the Centre for Counter Fraud Studies (CCFS 2017), in collaboration with Crowe Clark Whitehill and Experian, updated the fraud indicator estimate for the private sector, reducing estimated losses to £140b, due to the reduction in procurement expenditure by large UK companies. In business expenditure, the rate of procurement fraud was 4.76 percent and the rate of payroll fraud was 1.7 percent. Financial sector sales fraud was estimated to be £5.2b for 2017. The estimated total loss for individual victims of identity fraud was £1,344m in 2017. No specific estimates were provided for the costs of identity fraud for the private sector.

Cyber Security Breaches Survey (UK)

Official statistics from the UK government were obtained from a telephone survey of 1,523 UK businesses and 30 follow-up interviews (Klahr et al. 2017). Included were a number of cybercrime types that entailed misuse of identity (eg fraudulent emails or being directed to fraudulent websites, and impersonating organisation in emails or online).

The most prevalent category involved 'receiving fraudulent emails, or being directed to fraudulent websites' (72%), while for 27 percent of respondents the category was 'others impersonating the organization in emails or online' (Klahr et al. 2017: 41). However, almost 60 percent of respondents reported 'no significant impact' and that 'the median cost of all breaches was zero'. The most disruptive breaches involved a mean loss of approximately £1,220 for businesses with fewer than 50 employees and approximately £4,270 for those with 250 or fewer employees (Klahr et al. 2017: 47).

Impact of cybercrime on businesses (Belgium)

In 2017, an interdisciplinary study funded by the Belgian Science Policy Office examined the impact of cybercrime on Belgian businesses (Paoli et al. 2017). Five categories of cybercrimes that target businesses were examined, each of which could have an element of misuse of identity, although the two categories 'illegal access to IT systems' and 'Internet fraud' were the most likely to involve misuse of identity. The remaining three ('corporate espionage', 'data and system interference' and 'cyber extortion') were less likely to entail identity crime elements.

The study is important in that it adopted a novel methodology to assess harm by including various types of personnel costs in responding and repairing systems, as well as indirect harms such as damage to reputation and privacy—which have particular relevance to identity crime arising from data breaches and unauthorised access to data.

The survey comprised an online questionnaire completed by 453 representative Belgian businesses in a population of 9,249. Of the responses, 310 were analysed (3.4% of the population).

Victimisation rates were found to be high: 67 percent of all respondents reported being a victim of at least one of the five types of cybercrime; 50 percent experienced illegal access; 13 percent experienced internet fraud (36% experienced data/system interference, 24% cyber extortion and 4% cyber espionage).

Reported staff costs for neutralising incidents were quite low, with more than 70 percent of businesses experiencing illegal access reporting costs not higher than €229. For illegal access, more than 90 percent of businesses reported paying no fines or compensation to injured parties.

Of all the victims of illegal access, 72 percent suffered no revenue loss. However, illegal access affected internal operations, services to customers, reputation and privacy.

The study concluded:

> “…in a nutshell, business-related cybercrime occurs frequently but as of summer 2016, it did not generate serious costs or harm for the majority of businesses based in Belgium. (Paoli et al. 2017: 6)

The study is important in that it records findings ‘that are more conservative than those reported by private security and consultancy companies’ (Paoli et al. 2017: 6).

Impact of fraud on small businesses (Canada)

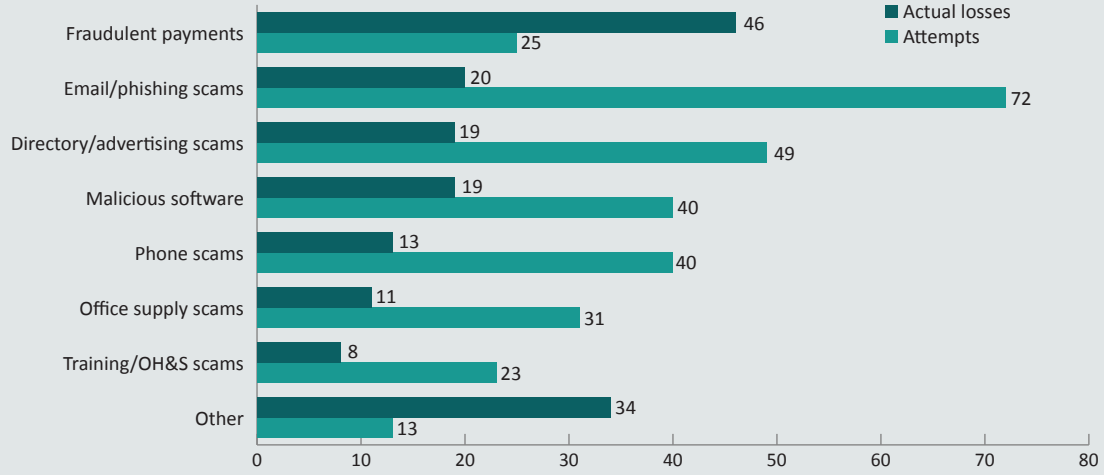
In March 2016, the Canadian Independent Federation of Business released a report outlining the impact of fraud on small businesses in Canada (Bourgeois & Gormanns 2016). Some of the key findings in the report included:

- One out of every five small business owners in Canada had been a victim of fraud in 2015, costing on average CA$6,200 per business.
- The most common scams to hurt small businesses were fraudulent payments, email scams and directory fraud.
- Small businesses spent an average of CA$2,900 on fraud prevention in the last year.
- Most small business owners reported that the stress and hassle of fraud were worse than the financial losses.
- Of the small businesses victimised by fraud, 44 percent did not report the fraud.

Fraudulent payments were by far the most common fraud type that caused a loss (Figure 1). One in five victimised small businesses were scammed by emails and phishing designed to trick them into providing sensitive information or transferring money. This was by far the most common type of attempted fraud on small business.

Other common scams that resulted in a loss were malicious software (eg malware, spyware or ransomware) and directory fraud or fraudulent advertising scams where payment is demanded for a product or service that was never ordered (eg bogus magazine ads or phone directory listings). One third of victims reported being defrauded by other scams, such as paying for goods or services that are never received; compromise of business credit cards or cheques; use of fraudulent identities (eg when applying for credit), identity theft and charity scams. Other commonly attempted scams included directory fraud, use of malicious software, and phone scams.

Figure 1: Types of attempted fraud versus types of fraud that victimised small businesses during the past 12 months in Canada (%)



Note: Includes only scams that involved attempts to defraud small businesses (light green) or scams that resulted in loss of money, goods, services or valuable information (dark green) in the last 12 months.

Source: Bourgeois & Gormanns 2016: 5

Global Fraud and Risk Report 2017–18 (Kroll)

Kroll's 2017–18 Global fraud and risk report (2018) involved an online survey of 540 senior executives from 10 industry sectors conducted globally in June–August 2017. It was found that information theft, loss or attack was the most prevalent type of fraud experienced in the preceding 12 months, reported by 29 percent of respondents (Kroll 2018: 6). Of the cyber attacks reported, 33 percent involved email-based phishing attacks. Across industry sectors, the percentages of respondents who reported fraud in the preceding year relating to information theft, loss or attack varied between 21 and 39 percent (Kroll 2018; see Table 8 below).

Approaches to costing

A variety of methodological approaches can be used to quantify the size and cost of a specific type of crime. At the outset, consideration needs to be given to what could be called 'the disaggregation problem'. Arguably, identity crime is not a unitary crime type; rather, it is a method of committing crime—specifically, fraud.

For this reason, Levi and Burrows (2008: 12) decided not to attempt to cost identity fraud as a 'victim of crime' type but instead treat it as a 'method of committing' fraud. If one agrees with this approach, then the starting point in costing identity crime would be to estimate the cost of fraud and then disaggregate the findings in terms of how fraud is committed. There are two difficulties with such an approach. First, identity crime involves more types of criminalities than fraud alone; second, few datasets include the method of commission as a variable. Further, for the purposes of this study, an additional variable—that is, the identity of the victim as a business enterprise—needs to be included, which is rare in prior research.

Disaggregating the cost of identity crime for business victims ($1,426m)

The 2017 *Identity crime and misuse in Australia* report (Jorna & Smith 2018) provided a basis for disaggregating the total estimated cost of identity crime and misuse to determine the proportion that was experienced by businesses in Australia. This can be achieved by taking the current estimate of the total cost of identity crime and misuse and removing those elements that do not involve Australian businesses.

Conventional costs of crime estimates have used the following classification of cost elements, which were also used for the 2017 *Identity crime and misuse in Australia* report (Jorna & Smith 2018).

Direct costs are losses actually incurred as a result of victimisation (the net losses after recovery of insurance, refunds or compensation are referred to as out-of-pocket costs), comprising:

- *amount obtained*—the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, credit, loans or cash;
- *additional costs*—those incurred by the victim as a result of misuse, or attempted misuse, of personal information, including legal fees, bank fees on dishonoured cheques or funds transfers, and other miscellaneous expenses such as postage, phone calls and court costs; and
- *less recoveries*—amounts recovered from offenders and any compensation and insurance payments made to victims.

Indirect costs fall into four principal categories:

- *prevention costs,* sometimes known as defensive expenditure, including items such as document security, computer security software, conducting credit checks, awareness-raising and prevention information, legislative and policy development by government, and other security measures to guard against victimisation;
- *intangible impacts* that cannot easily be measured in monetary terms, such as costs associated with mental and emotional harm and reputational damage;
- *response costs,* including expenses associated with dealing with the consequences of victimisation, such as repairing a credit rating, re-issuing credentials, reinstating systems, reporting to official agencies, and liaising with police and regulatory agencies in their investigations; and
- *lost output,* including lost opportunity costs and business disruption costs due to the misuse of personal and business information.

Column 4 of Table 7, below, shows the direct costs of fraud derived from the *Identity crime and misuse in Australia* report's estimate of the total direct costs of identity crime in 2015–16. These direct costs include actual amounts obtained by offenders as well as additional costs paid by victims of identity crime.

The additional direct costs component shown in column 4 of Table 7 is based on United States Bureau of Justice Statistics data for 2014, updated and converted to Australian dollar values for 2016 using purchasing power parities (PPP) constructed by the Organisation for Economic Co-operation and Development (OECD). Purchasing power parity is the exchange rate needed to equalise the purchasing power of two currencies in their respective countries (OECD 2018). Australia's rate in 2014 was approximately A$1.45, meaning one would need to spend A$1.45 in Australia to buy the quantity of goods or services that would cost US$1 in the United States. Using the expert panel's estimates of the percentage of these costs attributable to businesses, an estimate of the direct cost of identity crime to businesses was found to be $1.3b.

Analysis of the 2017 *Identity crime and misuse in Australia* report (Jorna & Smith 2018) results found that indirect costs of prevention and response to fraud by the private sector were $1.3b, of which 4 percent was estimated by the expert panel to relate to identity crime ($52.3m). This relied on Mayhew's (2003) estimate that 40 percent of direct fraud losses should be added to account for prevention and response costs, lost output and intangible losses. This was applied to the above estimate of $3.3b to give a total of $1.3b. Only four percent of this was estimated by the expert panel to be reasonable prevention and response costs in connection with identity crime.

Adding the direct and indirect costs to business of identity crime results in a total impact of $1.4b for 2015–16. Inflated to 2016–17 values using the Reserve Bank's (2018) calculator, the total is $1.426b.

Table 7: Business identity crime financial impact calculations, 2016–17

Category 2015–16 cost	Obtained identity cost ($)	Additional identity cost ($)	Total direct identity cost ($)	% business[a]	Total business identity cost ($)
Commonwealth entities	90,046,711	123,477	90,170,188	2 (2)	1,803,404
Individuals	234,955,384	4,113,302	239,068,686	5 (2)	11,953,434
Serious fraud	259,603,838	7,530	259,611,368	90 (3)	233,650,231
Police recorded	1,463,624,935	6,435,135	1,470,060,070	75 (1)	1,102,545,053
Total	2,048,230,868	10,679,444	2,058,910,312	–	1,349,952,122
Indirect business identity costs[b]	–	–	–	–	52,322,146
Total business impact of identity crime 2015–16	–	–	–	–	1,402,274,268
Inflated to 2016–17 dollars	–	–	–	–	1,426,228,168

a: Numbers in parentheses are confidence ratings: 3=high certainty, 2=medium certainty, 1=low certainty
b: The expert panel assessed only four percent of indirect business costs were attributable to identity crime
Source: Jorna & Smith 2018

Global GDP analysis ($1,967m)

A second approach to estimating the indirect costs of identity crime and misuse is to quantify the proportion of business output lost. The Centre for Counter Fraud Studies (2017) recently undertook an assessment of the global cost of fraud, based on estimates of the percentage of business expenditure lost to fraud annually. The study reported a mean loss of 5.85 percent. This model of estimation is argued to be more accurate than other models that attempt to extrapolate mean losses actually detected and experienced by applying a multiplier to the accounts for undetected and unreported crime (usually using a 25 percent multiplier in the case of fraud). The Centre for Counter Fraud Studies (2017) analysed 558 costing exercises that, over the preceding 19 years, sought to measure the financial cost of fraud and error. The exercises took place across 40 different types of expenditure, in 48 organisations from 10 countries, and considered losses in expenditure with a total value of £13.27 trillion.

The Centre for Counter Fraud Studies (2017: 8) found the range of percentage losses across all the exercises reviewed between 1997 and 2016 to be 'between 0.02 percent and 27.15 percent, with average losses of 5.85 percent (68% of the exercises showed loss figures of more than 3%)'. The global average loss rate for the entire period of the research (5.85%), when taken as a proportion of global GDP for 2016 ($75.212 trillion, or £60.76 trillion), equates to £3.55 trillion ($4.39 trillion).

In Australia, applying the global average fraud loss rate of 5.85 percent to Australian GDP in 2017 ($1,421,809,000,000) amounts to $83,175,826,500.

If it is assumed that identity crime and misuse is involved in 15 percent of all fraud and that 10 percent of this relates to business losses, then 1.5 percent of all fraud would involve business identity crime. Applying 1.5 percent to the estimated Australian fraud losses of $83b, the estimated cost to business of identity crime is $1,247,637,398. This excludes the cost of prevention and response, which could be expected to add an additional $720m, resulting in a total of $1,967,637,398. As a percentage of Australian GDP, the total impact of identity crime and misuse would be 0.1 percent.

Analysis based on industry value added ($1,799m)

Simply estimating the percentage of GDP that may be lost to fraud and then applying a further estimate of the percentage of fraud that may involve identity crime and misuse is an overly general way to estimate the cost of identity crime and misuse. This is because some businesses have much higher exposure to fraud and identity crime than others. A more precise approach would be to determine the contribution to GDP of businesses within each sector and then estimate their exposure to risk of identity crime.

In Australia, the ABS (2017a) publishes a measure of the contribution that businesses in each industry sector make to GDP, known as industry value-add (IVA). This is a more appropriate measure than business income, expenditure, turnover, or profit or loss, as it indicates the extent to which the sector contributes to GDP and thus the amount of GDP at risk owing to fraud and identity crime.

Table 8 presents estimates of the components of IVA for all industries that are within the scope of the collection. There are two types of businesses: 'market' and 'non-market' producers. Market producers sell their output to achieve a profit, whereas non-market producers sell their output at economically insignificant prices. IVA is derived differently for market and non-market producers. The industries in which non-market producers make the most significant contribution to IVA are health care and social assistance (private) and other services.

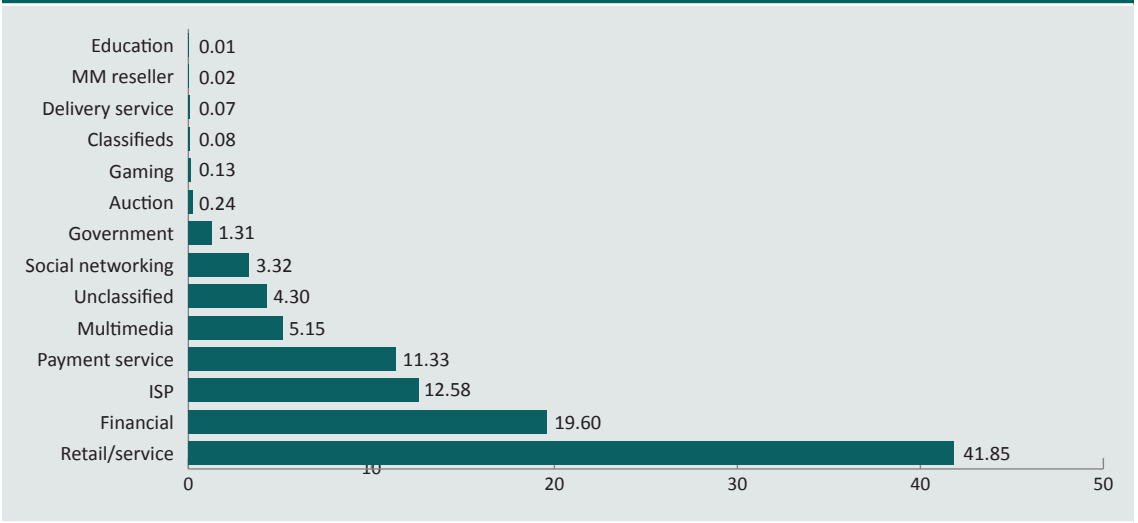
In addition to indicating the number of Australian businesses in each sector at 30 June 2016, and the corresponding IVA, Table 8 shows four indications of risk of identity crime. First is the number of security incidents reported by Verizon (2017) for 2016 and the per capita cost of data breaches in Australia reported by Ponemon (2017: 9):

> Although a small sample size prevents us from generalising industry cost differences, financial, services and technology companies tend to have a per capita cost higher than the mean ($139). In contrast, companies in the public sector, transportation and retail had a per capita cost significantly below the mean.

In addition, Kroll in its *Global fraud and risk report* (2018) reports the findings of its survey of senior executives on their industries' experience of 'information theft, loss or attack' during the preceding year. Although these data are not indicative of one industry being more or less secure than another, they do provide a metric of risk of identity crime in the relevant sector and have been used to estimate percentages of identity crime out of IVA cost.

Table 8 also shows the percentage of phishing attacks in some sectors reported by the Anti-Phishing Working Group (APWG 2017). These findings can be explained more fully by examining research conducted by MarkMonitor, a software company specialising in enterprise brand protection and one of the contributors to the APWG's Activity Trends reports. In 2016, MarkMonitor found that companies in the retail and financial services sectors remained the top targets for phishing (APWG 2017). Other findings from APWG (2017) are shown in Figure 2.

Figure 2: Most targeted industry sector to phishing, 4th quarter 2016 (%)



Source: Adapted from APWG 2017

Table 8 also shows findings from ACSC (2016: 9) incident reports for selected categories of businesses for 2015–16. It should be noted that ACSC categories do not precisely match ABS categories; accordingly, the table provides only a general indication of the numbers of incidents for some business types.

Using these data on security breaches, cyber incidents and phishing risk, in conjunction with the results of other industry research on fraud and identity crime risk (see *References*), it is possible to estimate the percentage of businesses in each sector that might have experienced identity crime and misuse, and to use this percentage to estimate the percentage of IVA lost to this crime type (columns 7 and 8, Table 8).

For the financial and insurance sector, the ABS (2017a) notes that estimates for Australian and New Zealand Standard Industrial Classification (ANZSIC) subdivision 64, 'Auxiliary finance and insurance services' for 2015–16 are experimental and subject to evaluation and should be used with caution. It may, therefore, be appropriate to add to this the fraud loss estimate provided by AusPayNet (2017) for payment system fraud (see *Payment system fraud in 2016*, above).

On the basis of this method of estimation, business losses to identity crime and misuse in Australia in 2016 would be in the region of $1.08b. This excludes the cost of prevention and response, which could be expected to add an additional $720m, totalling $1,799m.

Table 8: Estimates of industries' IVA components and indications of risk of identity crime

Division	Number	Data breaches (n) [a,f]	Cyber-security incidents (%)[e]	Phishing (%) [b] (APWG)[c]	Info theft (%) (Kroll 2018)[g]	Value add ($m)	Identity crime (%) and rating	Value identity crime ($m)
Agriculture, forestry and fishing	177,012	11	–	–	–	32,097	0.01 (1)	3.2
Mining	7,915	6	8.6	–	–	102,549	0.01 (1)	10.3
Manufacturing	83,585	620 ($142)	2.2	13.4	33	100,109	0.03 (2)	30.0
Electricity, gas, water and waste services	6,306	32	20.9	–	–	45,295	0.01 (1)	4.5
Construction	358,466	6	–	–	33	116,697	0.01 (1)	11.7
Wholesale trade	77,984	20	–	–	39	65,392	0.02 (1)	13.1
Retail trade	131,150	326 ($106)	1.9	10.7 (41.9)	21	75,500	0.08 (3)	60.4
Accommodation and food services	90,284	215	2.6	9.7	–	40,558	0.07 (1)	28.4
Transport, postal and warehousing	133,093	63 ($102)	10.3	–	34	72,079	0.01 (1)	7.2
Information media and telecommunications	20,024	717 ($145)	17.7	10.8	35	37,555	0.04 (2)	15.0
Auxiliary financial and insurance services[d]	193,489	998 ($232)	17	8.5 (19.6)	27	27,737	0.9 (3)	249.6
Rental, hiring and real estate services	240,509	13	–	–	–	79,000	0.03 (1)	23.7
Professional, scientific and technical services	262,133	3,016 ($157)	2.4	–	33	108,371	0.05 (2)	54.2
Administrative and support services	82,410	42 ($201)	–	–	–	54,138	0.01 (1)	5.4
Public administration and safety	7,288	21,239 ($67)	5.5	9.2	–	5,533	0.09 (2)	5.0

Table 8: Estimates of industries' IVA components and indications of risk of identity crime

Division	Number	Data breaches (n) [a,f]	Cyber-security incidents (%)[e]	Phishing (%) [b] (APWG)[c]	Info theft (%) (Kroll 2018)[g]	Value add ($m)	Identity crime (%) and rating	Value identity crime ($m)
Education and training	28,399	455 ($140)	2.6	6.2 (0.01)	–	27,988	0.08 (1)	22.4
Health care and social assistance	123,416	458	1.9	10.3	23	79,455	0.02 (1)	15.9
Arts and recreation services	26,418	5,534 ($113)	–	–	–	12,635	0.03 (1)	3.8
Other services (media)	91,571	77 ($121)	6.4	–	–	28,914	0.01 (1)	2.9
Currently unknown	30,092	8,220	–	–	–	–	–	–
All industries	2,171,544	42,068	–	–	–	1,083,865	0.20 (1)	566.7
Payments industry[h]	130	–	–	–	–	540	0.95 (3)	513
Total	–	–	–	–	–	–	–	**1,079.7**

Note: Ratings: 3=high certainty, 2=medium certainty, 1=low certainty

Sources:

a: Verizon (2017: 9), number of security incidents in 2016

b: Verizon (2017: 9), number of security incidents in 2016 involving phishing

c: APWG (2016), percentage of phishing attacks in sector

d: ABS (2017a: Table 1). Estimates for ANZSIC Subdivision 64 Auxiliary finance and insurance services for 2015–16 are experimental and subject to evaluation and therefore should be used with caution

e: ACSC 2016: 9 (n=14,804). ACSC categories do not precisely match ABS categories

f: Figures in parentheses are per capita data breach costs in Australia for 2017 in A$ (Ponemon 2017: 9). Ponemon's categories do not precisely match ABS categories

g: Kroll (2018). Fraud type, information theft, loss or attack (data theft) % reported in previous year

h: AusPayNet (2017)

Summary and conclusions

This study sought to estimate the current extent and financial impact of identity crime and misuse affecting the Australian business sector. The challenges in undertaking such an enterprise should not be underestimated, as baseline data on crime against Australian businesses are limited, and information on the proportion of crime that involves criminal misuse of identity is even more restricted. As such, a number of methodologies to estimate the scale of the problem had to be developed that, unfortunately, were unable to completely address the missing data needed to arrive at a precise conclusion.

At 30 June 2016, Australia had almost 2.2m businesses, including a very small proportion of large public corporations. Over 60 percent were small businesses with a single proprietor. Data from overseas indicate that fraud disproportionately affects these small enterprises (National Fraud Authority 2013). It is to be expected that identity crime and misuse also occurs more often in small organisations.

Existing Australian data on the cost of identity crime and misuse are selective and variable in scope, reliability and focus. The most reliable source concerns payment system fraud, almost all of which entails misuse of personal information. This amounted to $540m in 2016 (AusPayNet 2017).

Consumer scams targeting businesses that were reported to Scamwatch in 2017 involved losses of $4.7m, of which $1.8m might have involved business-related identity crime. Inflating this estimate to account for unreported matters, it is likely that businesses lost $3.6m to identity crime scams in 2017.

ACORN reports in 2016 of online scams involving identity crime affecting organisations involved approximately $130.2m, inflating costs to account for unreported matters—but almost all of these would be counted as part of payment system data and Scamwatch reports.

Other data sources, such as from CERT Australia (ACSC 2015) and the Small Business Scam Survey (Weber & Geneste 2012), do not provide loss estimates for business-related identity crimes.

In order to provide a more comprehensive estimate of identity crime losses that affect the whole Australian business sector, a number of methodologies were used, following approaches developed in the UK and Europe. In the absence of nationally representative, actual business victimisation survey data in Australia, the estimates described above indicate potential losses from business identity crime in 2017 of between $1.4b and $2.0b, or an average of the three estimates of $1.7b, as follows:

- disaggregation of the existing estimate of the financial impact of identity crime in Australia that relates to business victimisation ($1.426b);
- application of percentages of GDP that could relate to fraud and identity crime in particular ($1.967b); and
- determining the proportion of IVA that could entail identity crime and misuse ($1.799b).

However, these estimates are heavily dependent on estimates of the proportion of business fraud losses and industry output that might entail identity crime and misuse. This study relied on estimates derived from the survey and other administrative data cited, assessed by a panel of industry and academic peer reviewers. Further efforts to verify these estimates, particularly in those sectors for which baseline information is lacking, await more rigorous study.

Nonetheless, the scale of the estimated losses that might be suffered by the Australian business sector requires further effort to reduce the risks of such harm. To date, a number of private sector and government organisations have established worthwhile information resources for businesses on how to prevent risks of identity crime and identify attacks in real time.

For example, the Australian Government (2017) provides advice to small businesses on how to adopt good security practices when conducting business online. The *Stay smart online small business guide* was developed in collaboration with the New Zealand Department of the Prime Minister and Cabinet, Australia Post, Australia and New Zealand Banking Group Limited, Commonwealth Bank, National Australia Bank, NBN, Westpac and Telstra, and is part of the government's Cyber Security Strategy.

Similarly, the ACCC (2017a) publishes a factsheet that provides specific information on business scams. *Business scams: Information for businesses* outlines the nature of the main scams directed at businesses, their method of attack, and what businesses should do to guard against them. In New South Wales, the Office of the Small Business Commissioner (2017) provides advice to small business owners on responding to cybercrime risks.

In the UK, similar resources are available online (eg the UK government's Cyber Aware website, and the business section of the Get Safe Online website). PROOF (Protected Online Filing) is a free online filing service established at Companies House (2018), which seeks to protect firms from the risk of identity theft. Once an organisation is registered with PROOF, only those with authentication codes issued by Companies House can file documents for the company (eg changes of address or bank accounts). These and other initiatives are reviewed in the City of London research report *The implications of economic cybercrime for policing* (Levi et al. 2015: 48–50). The website of the Canadian Federation of Independent Business also has advice for small businesses on fraud prevention.

Despite the existence of these resources, there remains a need for businesses—particularly small and micro enterprises—to understand the need to allocate resources to preventive measures. This is the case even though some preventive measures entail considerable financial burdens, such as improved computer hardware and software; ongoing maintenance; training of personnel; fraud awareness education; improved detection and monitoring systems, including data analytics and automated detection systems; and risk management and loss recovery solutions. In view of the current estimate that at least half of the total cost of identity crime and misuse in Australia is borne by the business sector, and most of that by small enterprises, there is a definite need for action.

In the United States, the National Association of Secretaries of State (NASS 2012) reviewed business identity theft and recommended establishing a task force to deal with the problem, similar to the Scams Awareness Network, which deals with consumer fraud against individuals (ACCC 2018). The approach taken by the National Association of Secretaries of State involved awareness-raising, legislative reform, data collection and sharing, training for law enforcement, centralised reporting, and victim support. Similar steps are needed in Australia to deal with an emerging problem that continues to affect the private sector.

References

URLs correct as at August 2018

Action Fraud 2018. United Kingdom National Fraud & Cyber Crime Reporting Centre. https://actionfraud.police.uk/

Anderson R, Barton C, Böhme R, Clayton R, van Eeten MJG, Levi M, Moore T & Savage S 2013. Measuring the cost of cybercrime, in Böhme R (ed), *The economics of information security and privacy.* New York: Springer: 265–300

Anti-Phishing Working Group (APWG) 2016. *Phishing activity trends report.* http://www.antiphishing.org

Attorney-General's Department (AGD) 2016. *Identity crime and misuse in Australia 2016.* Canberra: Attorney-General's Department

Australasian Centre for Policing Research (ACPR) 2006. *Standardisation of definitions of identity crime terms: A step towards consistency.* Report series no. 145.3. Adelaide: ACPR

Australian Bureau of Statistics (ABS) 2017a. *Australian industry by division, 2015–16.* ABS cat. no. 8155.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8155.0

ABS 2017b. *Counts of Australian businesses, including entries and exits, Jun 2012 to Jun 2016.* ABS cat. no. 8165.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/8165.0

ABS 2012. *Personal fraud, 2010–2011.* ABS cat. no. 4528.0. Canberra: ABS. http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0/

Australian Competition and Consumer Commission (ACCC) 2018. *Targeting scams: Report of the ACCC on scams activity 2017.* Canberra: ACCC

ACCC 2017a. *Business scams: Information for businesses.* Canberra: ACCC

ACCC 2017b. *Targeting scams: Report of the ACCC on scams activity 2016.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

Australian Criminal Intelligence Commission (ACIC) 2017. *Australian Cybercrime Online Reporting Network (ACORN) statistics 2016.* Canberra: ACIC

Australian Cyber Security Centre (ACSC) 2016. *Threat report 2016.* Canberra: ACSC

Australian Cyber Security Centre (ACSC) 2015. *Cyber security survey: Major Australian businesses.* Canberra: ACSC and CERT Australia

Australian Government 2017. *Stay smart online small business guide,* 2nd ed. Canberra: Australian Government. https://www.staysmartonline.gov.au/get-involved/guides/smallbusinessguide

Australian Payments Network (AusPayNet) 2017. *Australian payments fraud 2017.* Sydney: AusPayNet. http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-calendar-year-2016.pdf

Australian Securities and Investments Commission (ASIC) 2016. *ePayments Code.* Canberra: ASIC. http://asic.gov.au/regulatory-resources/financial-services/epayments-code/#download

Australian Securities and Investments Commission (ASIC) 2005. *Compliance with the EFT code of conduct.* Canberra: ASIC. http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-63-compliance-with-the-eft-code-of-conduct-april-2003-to-march-2004/

Bourgeois A & Gormanns N 2016. *Fraud: A big threat to small business.* Ottawa: Canadian Federation of Independent Business. http://www.cfib-fcei.ca/cfib-documents/rr3391.pdf

British Retail Consortium 2017. *2016 Retail crime survey.* London: British Retail Consortium

Burrows J, Anderson S, Bamfield J, Hopkins M & Ingram D 1998. *Counting the cost: Crime against business in Scotland.* Stirling: Scottish Business Crime Centre

Canadian Federation of Independent Business 2017. https://www.cfib-fcei.ca/en

Centre for Counter Fraud Studies (CCFS) 2017. *Annual fraud indicator 2017.* London: University of Portsmouth, Crowe Clark Whitehall and Experian. https://www.croweclarkwhitehill.co.uk/wp-content/uploads/sites/2/2017/11/Annual-fraud-indicator-2017.pdf

Centre for Counter Fraud Studies (CCFS) 2016. *Annual fraud indicator 2016.* London: University of Portsmouth, Experian and PKF Littlejohn

City of London Police 2016. *Over £45 million lost by businesses in the City of London to online crime in the last year.* https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/nfib-news/pages/over-45-million-lost-by-businesses-in-the-city-of-london.aspx

Companies House 2018. PROOF (Protected Online Filing). http://www.companieshouseonline.com/index.php/homepage/information-f-a-q/87-proof-protected-online-filing

Department of the Prime Minister and Cabinet (DPM&C) 2016. Australia's cyber security strategy: Enabling innovation, growth & prosperity. Canberra: DPM&C. https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf

Financial Fraud Action UK 2016. *Fraud the facts 2016: The definitive overview of payment industry fraud.* https://www.financialfraudaction.org.uk/publications/

Get Safe Online 2018. https://www.getsafeonline.org/

Jorna P & Smith RG 2018. *Identity crime and misuse in Australia 2017.* Statistical Report no. 10. Canberra: Australian Institute of Criminology

Klahr R, Shah JN, Sheriffs P, Rossington T, Pestell G, Button M & Wang V 2017. *Cyber security breaches survey 2017.* London: Ipsos MORI and University of Portsmouth. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

KPMG 2013. *Fraud, bribery and corruption survey 2012.* Sydney: KPMG

Kroll 2018. *Global fraud and risk report 2017–18.* https://www.kroll.com/en-us/global-fraud-and-risk-report-2018#download

Levi M, Doig A, Gundur R, Wall D & Williams M 2015. *The implications of economic cybercrime for policing: Report and technical annex.* London: City of London Corporation

Macdonald W & Fitzgerald J 2014. *Understanding fraud: The nature of fraud offences recorded by NSW police.* Contemporary Issues in Crime and Justice No. 180. Sydney: NSW Bureau of Crime Statistics and Research

Mayhew P 2003. *Counting the costs of crime in Australia: Technical report.* Technical and Background Paper Series No 4. Canberra: Australian Institute of Criminology

National Association of Secretaries of State (NASS) 2012. *Developing state solutions to business identity theft.* Washington: NASS

National Audit Office 2017. *Online fraud: Report by the Comptroller and Auditor General.* https://www.nao.org.uk/report/online-fraud/

National Fraud Authority 2013. *Annual fraud indicator.* London: National Fraud Authority

New South Wales Small Business Commissioner 2017. Presentation to the Australasian Consumer Fraud Taskforce, 24 February.

Organisation for Economic Co-operation and Development (OECD) 2018. *Purchasing power parities (PPP).* https://data.oecd.org/conversion/purchasing-power-parities-ppp.htm

Paoli L, Visschers J, Verstraete C & van Hellemont E 2017. *The impact of cybercrime on Belgium businesses.* Leuven: KU Leuven

Ponemon Institute 2017. *Cost of data breach study: Australia*. Michigan: Ponemon Institute

Reserve Bank of Australia (RBA) 2018. Inflation calculator. http://www.rba.gov.au/calculator/

Richards K 2008. *The Australian business assessment of computer user security: A national survey.* Research and public policy series no. 102. Canberra: Australian Institute of Criminology

Schaper M T & Weber P 2012. Understanding small business scams. *Journal of Enterprising Culture* 20(3): 333–56

Veda 2016. *Cybercrime and fraud report.* Sydney: Veda Advantage Information Services & Solutions Ltd

Verizon 2017. *Data breach investigations report.* http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

Walker J 1994. *The first national survey of crimes against businesses.* Canberra: Australian Institute of Criminology

Warfield B 2013. *Employee fraud in Australian financial institutions.* Sydney: Warfield & Associates

Weber P & Geneste L 2012. *Small business scams survey.* Perth: Curtin University

Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology and Professor in the College of Business, Government and Law at Flinders University.

Appendix

Table A1: Summary data: Australian business victims of fraud and identity crime research

Author (year)	Title	Method	Location	Period	Sample size	Reported loss ($)	ID crime type (n)	Reported ID cost	Total ID cost ($)
AusPayNet (2017)	Payment Fraud Statistics	Reported fraud incidents	Australia	2016	n.s.	540m	2.8m Transactions	$540m	540m
ACCC (2018)	Targeting scams (businesses)	Online victim Reports	Australia	2017	5,432 reports	4,669,409	Estimate	$1,810,861	3.6m
ACORN (2016)	ACORN business statistics	Cybercrime self-reports	Australia	2016	4,071 business reports	218m	81	$43,391,598	130.2m
ACSC (2017)	Cyber Security Survey	Major businesses	Australia	2015–16	149 organisations	n.s.	23% info breaches	n.s.	n.s.
Weber & Geneste (2013)	Small business scams survey	Online business survey	Australia	2012	192	100–10,000 Mean =1,258	72% victims	11.9% actual losses	318.7m
Warfield (2013)	Employee fraud in financial institutions	Court decisions	Australia	2000–13	120 cases	271,266,481	5 x credit card fraud	$2,375,489	–
Ponemon (2017)	Cost of data breach (businesses)	Data breach analysis by interview	Australia	2015–16	26	2.64m	potential	2.64m	
Veda (2016)	Cybercrime and fraud	Victim survey (consumers)	Australia	2015–16	2.5m	>2b	12m lifetime	11% 27%	

Table A1: Summary data: Australian business victims of fraud and identity crime research

Author (year)	Title	Method	Location	Period	Sample size	Reported loss ($)	ID crime type (n)	Reported ID cost	Total ID cost ($)
Richards (2009)	ABACUS business survey	Business survey	Australia	2008	4,000	595m–649m	n.s.	n.s.	–
Macdonald & Fitzgerald (2014)	BOCSAR Understanding fraud	Police fraud offences	NSW	2008–13	1,000 cases	20m total losses	ID theft 23 victims	$33,529	–

AIC reports

Research Report

Australia's national research and knowledge centre on crime and justice

aic.gov.au