Scams are now bigger business than Payments Fraud

September 2020

David Ojerholm

Lance Blockley

The Initiatives Group

Is there anything familiar about these?

"We represent a senior official in the Nigerian Government who wishes to transfer US$18 million	*"I am from the Her Majesty's Revenue and Customes in the UK. Your tax refund is now"*	*"You have been named as a beneficiary in a will and stand to receive a significant sum. Please contact us urgently"*

The unanimous response is *"yes, have heard that all before".* They are all phishing for financial information that can allow them to take over an identity/bank account and, by having the correct information, make and receive payments. And, believe it or not, they impact sophisticated and unsophisticated victims alike.

Payments Scams – what are they?

In setting the scene, it is important to recognise the difference between Payments Scams and Payments Fraud.

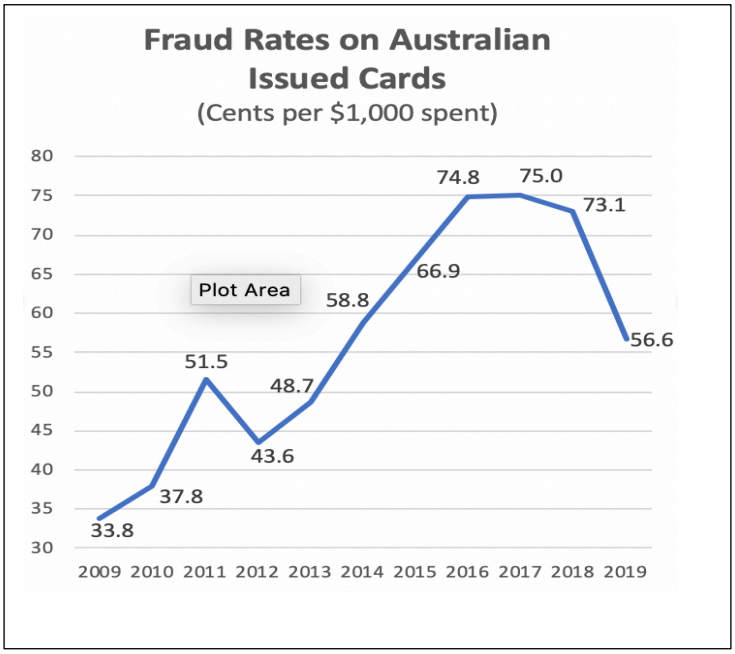
Historically, Payments Fraud has been defined as an *unauthorised* payment on an account made by a third party, the fraudster; that is, the account holder did not authorise for that payment to be made. Whereas a Payments Scam has been defined as an *authorised* payment on an account made by the account holder themselves (and not by anyone else). Whilst the difference may seem "black and white", this is not necessarily the case.

Payments scams and payments fraud are different

Consider the difference between a scam where a customer is convinced that they are paying a legitimate person or company (but in reality it is an imposter/fraudster/criminal) and authorises the payment themselves, versus a scam where a customer unwittingly/unknowingly provides information that enables a scammer to set up and then authorise a payment from the customer's account.

Both are induced by scams, however the first is legitimately authorised by the customer, whilst the second is authorised by the scammer (posing as the customer).

Payments Scams and Fraud are different, are they heading in the same direction?



No. As we explain in this paper, payments fraud is a growing industry whilst, thankfully, improvements in payments security (tokenisation, use of strong authentication, better fraud monitoring) has meant that the rate of payments fraud in Australia has begun to fall.

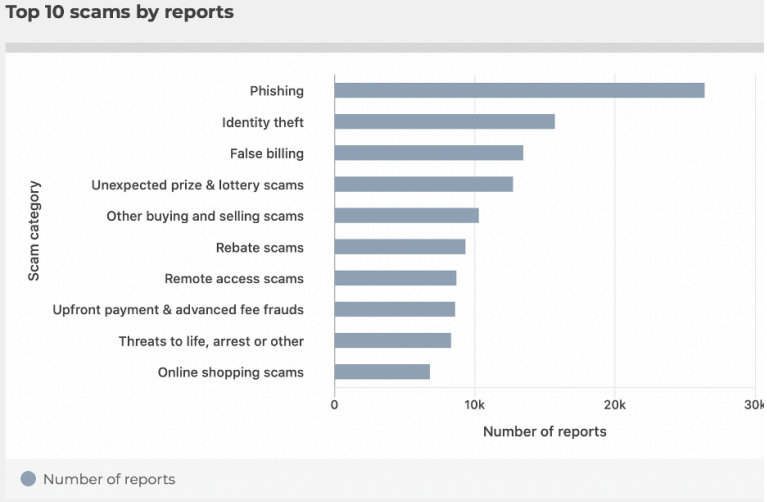
Fraud losses on Australian issued payment cards dropped for the last two years to levels last seen in 2014. Despite card transactions growing by 3.9% to over $819 billion, fraud losses dropped by 19% to $464 million. This is only 56.6c per $1,000 which is an excellent result.

What Payment Scams are most prevalent?

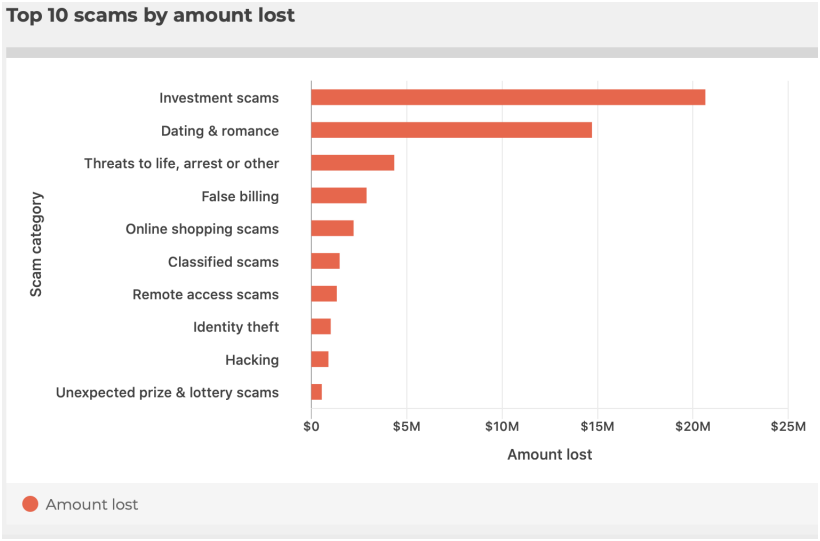
Looking at Australia, the Australian Competition & Consumer Commission (ACCC) has been tracking the rise of scams for some time.

The table opposite from the ACCC's Scamwatch[1] shows the top 10 types of scam reported by scam victims during the first half of 2020.

Phishing and Identity Theft are in the top 3, and, as noted above, these could result in payments being authorised by the criminal "impersonating" the account holder.



More important for this discussion are the top 10 scams by the amount of loss, shown in the second table. In fact, during the first 7 months of 2020, 13% of reported scams resulted in an actual financial loss[2].



Whilst the categories in this table appear straightforward, it should be noted that 4 of these did not appear in the same table published in 2017.

The arrival of "new" categories illustrates both how the scam environment is evolving and the difficulties in specifying appropriate definitions that clearly characterise the various forms of criminal activity.

Indeed, different countries use different terms; for example, FinanceUK brackets scams within two categories[3] –

1. Malicious Payee: within which Purchase scam, Investment scam, Romance scam and Advance fee scam are included; and
2. Malicious Redirection: covering Invoice & Mandate scam, CEO Fraud, Impersonation (most frequently police and bank staff), and Other.

---

[1] https://www.scamwatch.gov.au/scam-statistics?scamid=all&date=2020

[2] https://www.scamwatch.gov.au/scam-statistics

[3] https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-14-May.pdf

Is it a growth industry?

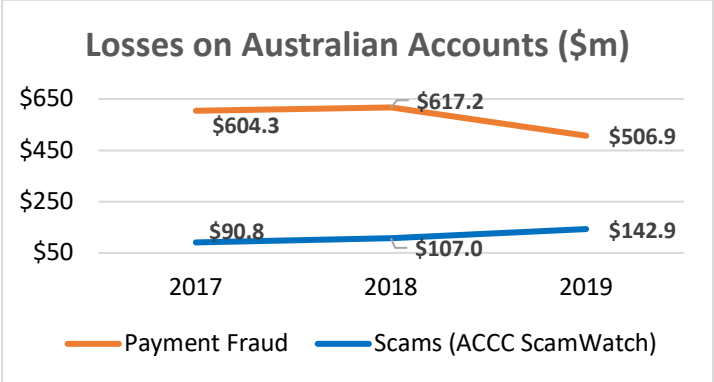
Yes, but not one you would choose to invest in.

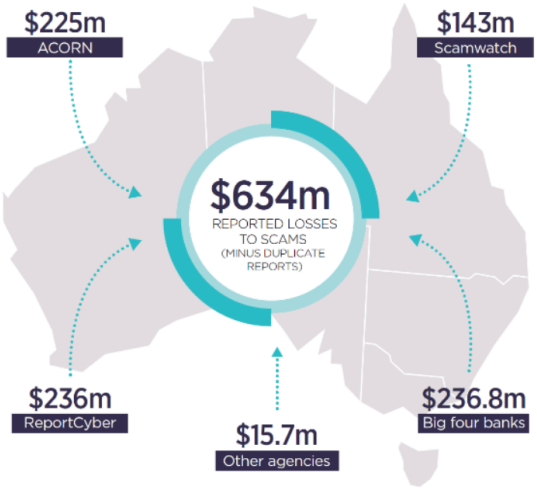
From January to July 2020 reported losses (from the 13,000 reported cases that resulted in financial loss) were $89.6 million, with an average value of almost $7,000. At a more granular level, whilst the total number of cases reported to the ACCC has not changed significantly since 2017, over the last 3 years the table below shows that:

- The proportion of scams which have involved financial loss has increased by 51%;
- The average loss in each incident has increased by 15%, from $6,462 to $7,449; and
- The total reported loss has increased by ~60% from $90.8m in 2017 to $143 million in 2019.

	Reported losses $millions	**Cases reported '000's**	**% with financial loss**	**Average loss**
2017	$90.8	161.5	8.7%	$6462
2018	$107.0	177.5	9.9%	$6089
2019	$142.9	167.8	11.8%	$7217
2020 (7 months)	$89.6	99.3	13%	$6938
2020 (annualised)	$153.6	170.3	13%	$6938

Comparing Payments Fraud with Payments Scams is also interesting reading. Whilst Payments Scams were only 28% of Payments Fraud in 2019, the value was a much smaller 15% in 2017 - the two are converging as the value of Scams continues to increase and the value of Fraud starts to rapidly decrease.

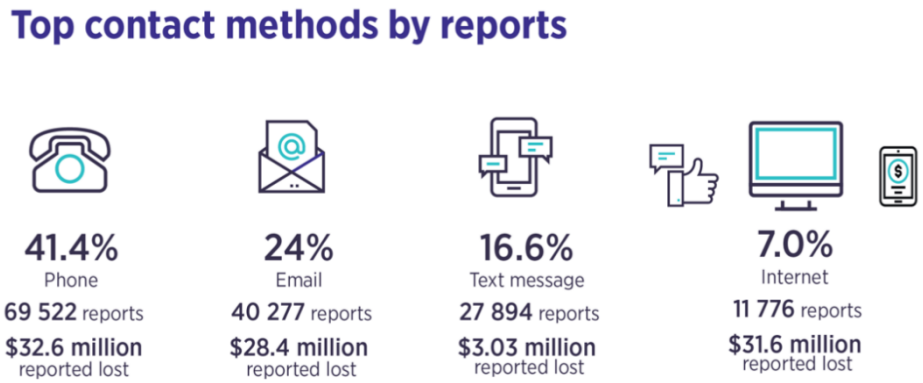




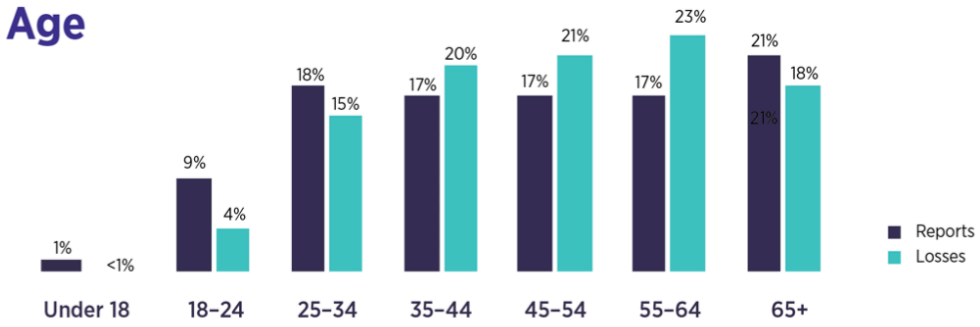
However, the ACCC Scamwatch is but only one of the various services to which Australian consumers and businesses can report scams, and the ACCC has valiantly led an effort to bring all of the information into one place. For 2019, this shows that total reported scam losses in Australia amounted to AUD634 million (a 30 per cent increase on 2018, when AUD489 million was reported lost), eclipsing the total amount of payments fraud occurring on Australian accounts.

How and who are popular with scammers?

Channels: Whilst over the years scammers have increasingly adopted electronic and social media channels, scamming by phone remains prevalent. ACCC Scamwatch has reported the following statistics for the proportion of scams, and the value scammed, by channel. Note that the average loss per scam is highest via the internet, followed by email:



Age Groups: Whilst some may think that it is the old who are most at risk, the ACCC statistics show that although they are the most targeted group, their losses are not much different to all age groups from 25 years old onwards:



Has Covid-19 had an impact?

Yes and no. The cost of financial scams continues to grow, however this does not appear due (at least solely) to the impact of Covid-19. Rather it has influenced the construct of the scam "scenarios" being played, rather than significantly accelerating losses.

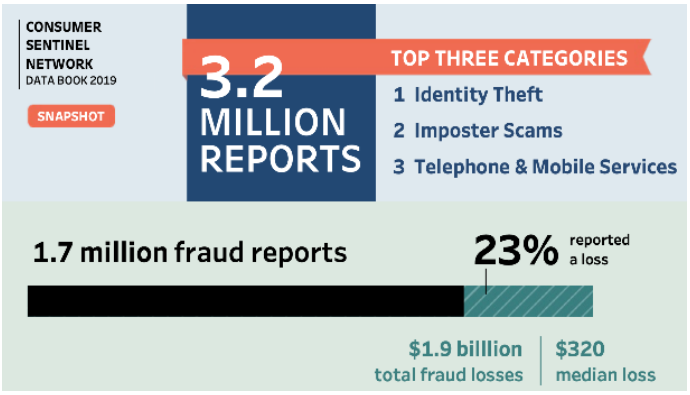
For example, fake government communications offering Covid-19 grants and relief funds, exploitation of the rapid growth in ecommerce and the use of subscription services, even offers for hand sanitisers and face masks that will never be delivered.

Is Australia unique?

No. Whilst scammers may or may not be global operators (which is certainly the case with payment fraudsters), scamming is a growing global "industry" with many common contact methods and scam methodologies used across multiple jurisdictions. Scam related financial losses are increasing just about everywhere. In the UK, the value of scam losses rose by 29% in 2019 compared to the prior year, with reported cases up 45% over the same period.[4]

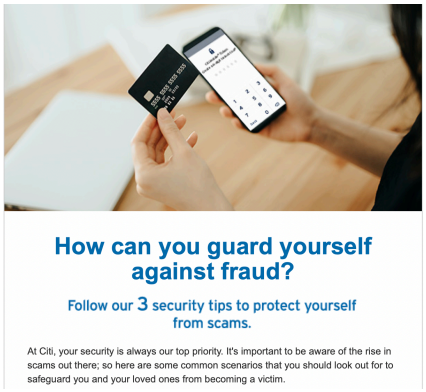
[4] https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-14-May.pdf

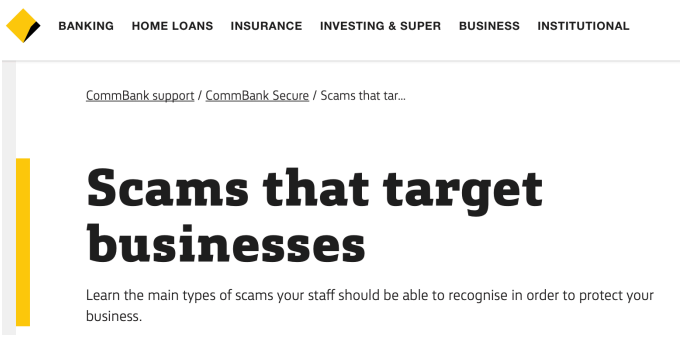
The table to the right shows the scam activity experienced in the USA in 2019, where the number of scam incidents increased by 21% and the value of losses rose by 28% as compared with 2018 data.[5] The top method for scammers contacting consumers was via phone[6]; it is the same in Australia, where the most common contact method for all scams is email, but phone has been the #1 contact method associated with scams that result in financial loss.

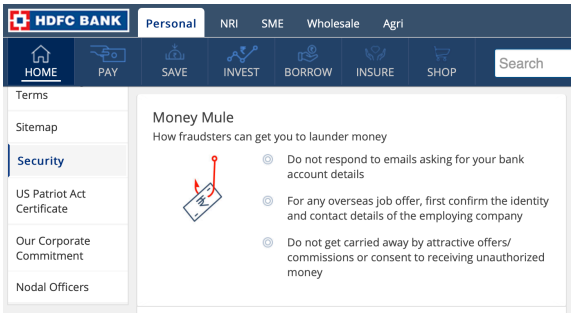


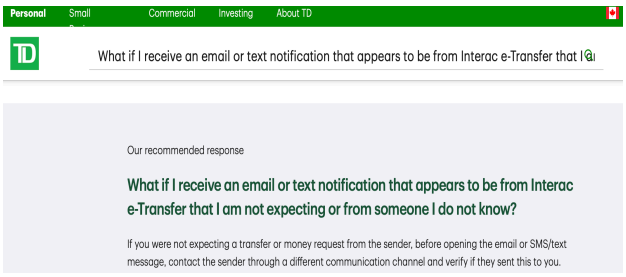
The action plan: Education, Awareness, Tracking

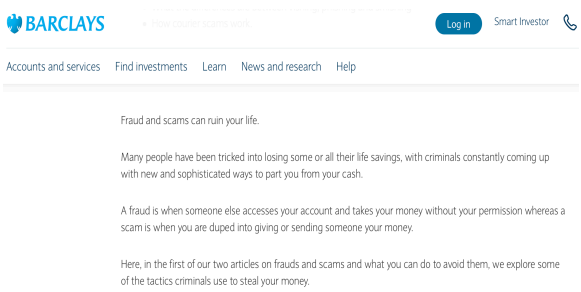
They say that every picture tells a story – that scamming is a global phenomenon is evidenced by the following images from Hong Kong, Australia, India, Canada, the UK and the USA.

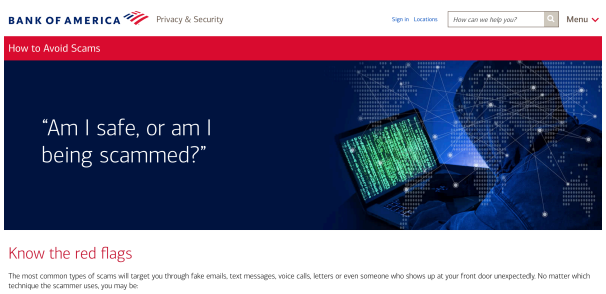












[5] https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018
[6] https://www.usa.gov/common-scams-frauds

In fact, it would be difficult to find a financial institution anywhere that does not have scam warnings/information on its website. In every jurisdiction and every example, financial institutions and government are undertaking efforts to educate their customers. In some instances, such as in the UK, the government has mandated that the banks are liable for customer losses. In all instances and jurisdictions, the banks are taking action to try and reduce the impact of scams.

Governments and financial institutions are taking on the responsibility to educate themselves, consumers and businesses regarding the types of scams and the circumstances scammers are exploiting in order to deceive account holders. Banks are doing more to identify account takeovers and to shut down "fake named" and "mule" accounts that scammers use to receive payments, but that may not stop payments being received in the first place and then immediately funnelled away to out-of-reach locations.

Consumers and businesses need to become more aware of any external efforts influencing them to authorise what might be a fraudulent/scam payment, and immediately report their suspicions to their bank and the relevant Government authorities. In Australia, this is the Australian Cyber Security Centre (https://www.cyber.gov.au).

One consistently strong message is that consumers need to protect their personal information. Scammers seek to steal money but, more often than not, their methods also involve the collection of personal information and data. Scammers use personal data to steal identities, open loans, and steal or launder money.

The ACCC[7] notes that a key pillar in scam prevention is the importance of telling others about scam experiences, or 'word of mouth'. Many people who avoided scams did so because their friends or family had told them about the scams, or that the approach or experience seemed suspicious. However, many people who have been scammed feel embarrassed by the experience ("How could I have been so stupid?"), but the sophistication of modern-day scammers is such that there is no need for such "shame" and victims would be helping others to avoid further crimes by speaking about their misfortunes.

Remember, if something is too good to be true or if a demand for payment appears overly unreasonable, then it probably is and should be either ignored or authenticated via separate communications. Stay safe.

[7] ACCC's "Targeting Scams 2019" publication

The Initiatives Group

The Initiatives Group - we help participants across the payments sector to generate more value from their markets and customers.

The consulting team at The Initiatives Group has advised participants in the payments market since the 1990's - including issuers, acquirers, third-party processors, technology providers and associations. We help solve many of the financial industry's most significant issues, such as payments strategies, customer profitability and retention, credit and fraud risk, leveraging new technologies, and assessing new market and product opportunities.

www.initiatives.com.au

Lance Blockley +61 418 479 027

David Ojerholm +61 418 233 677