Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**

WA ScamNet Year in Review

February 2020

Overview

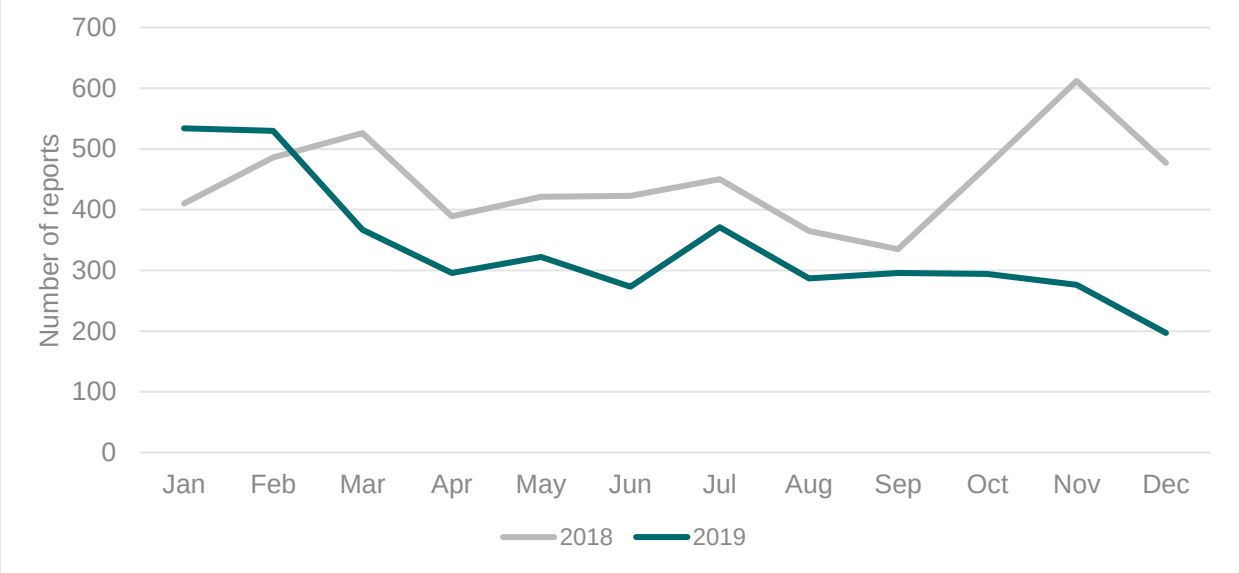
Each year, Consumer Protection receives a large number of enquiries concerning scam related problems. Many of these enquiries are lower level enquiries where consumers wish to advise Consumer Protection of an email, phone call or some form of interactions they have had with a potential scam. These types of enquiries are dealt with by Consumer Protection's Contact Centre. Other more detailed enquiries are managed by Consumer Protection's WA ScamNet team; these enquiries tend to be more detailed in nature often including situations where consumers have fallen victim to a scam and lost money, personal information, banking information or commercial information.

WA ScamNet uses the same scam categories used by the Australian Competition and Consumer Commission's (ACCC) ScamWatch to enable a comparison to be made between the reports received in WA and nationally.

Contact Centre

In 2019 Consumer Protection's Contact Centre received 4,043 calls relating to scams, 25 per cent fewer than in 2018. This was down from an average of 447 calls a month to 337 calls a month.

Figure 1. Scam reports received by the Contact Centre



The top three scams reported to the Contact Centre were the National Broadband Network scam (382 enquiries, 29 per cent increase from 2018), the Australian Tax Office Scam (342 enquiries, 39 per cent decrease from 2018) and the accident compensation scam (204 enquiries, 42 per cent decrease from 2018).

WA ScamNet

WA ScamNet receives reports of scams from several different sources including an Online Scam Reporting tool (OSR), referrals from the Contact Centre and through collaboration with Crime Stoppers WA, WA Police and other state and national government agencies. Although WA ScamNet receives calls about scammers from WA, other areas in Australia and overseas, the WA ScamNet Review document only focuses on reports and victims in WA.

The OSR was launched in April 2018 with data available from August 2018 (Figure 2). This tool allows people to report a scam to WA ScamNet that they have been a victim of, anonymously or on behalf of someone they know or a business. Data, including demographic information, is collected relating to the scammer, the victim and the type of scam. Other sources of information received by WA ScamNet do not include demographical information.

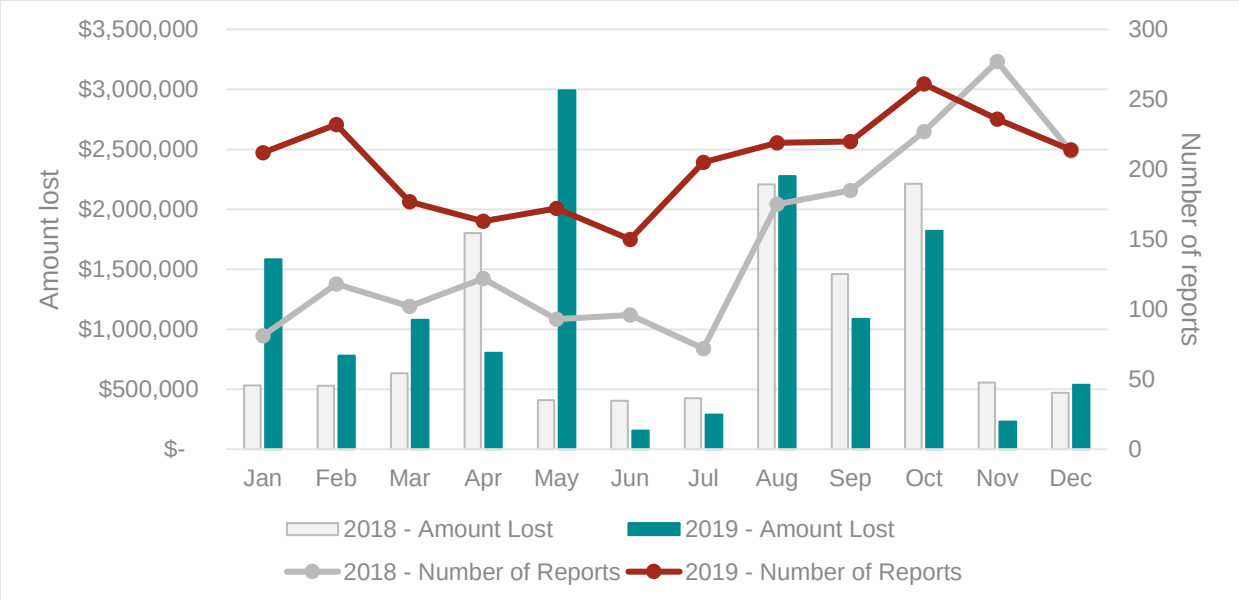
Losses

Table 1 shows the number of reports, and amounts lost, in 2019. This included three reported losses over $900,000 each lost to an investment scam (August 2019), romance scam (May 2019), and a payment redirection scam (October 2019).

Table 1. Statistics for reports to WA ScamNet for 2019

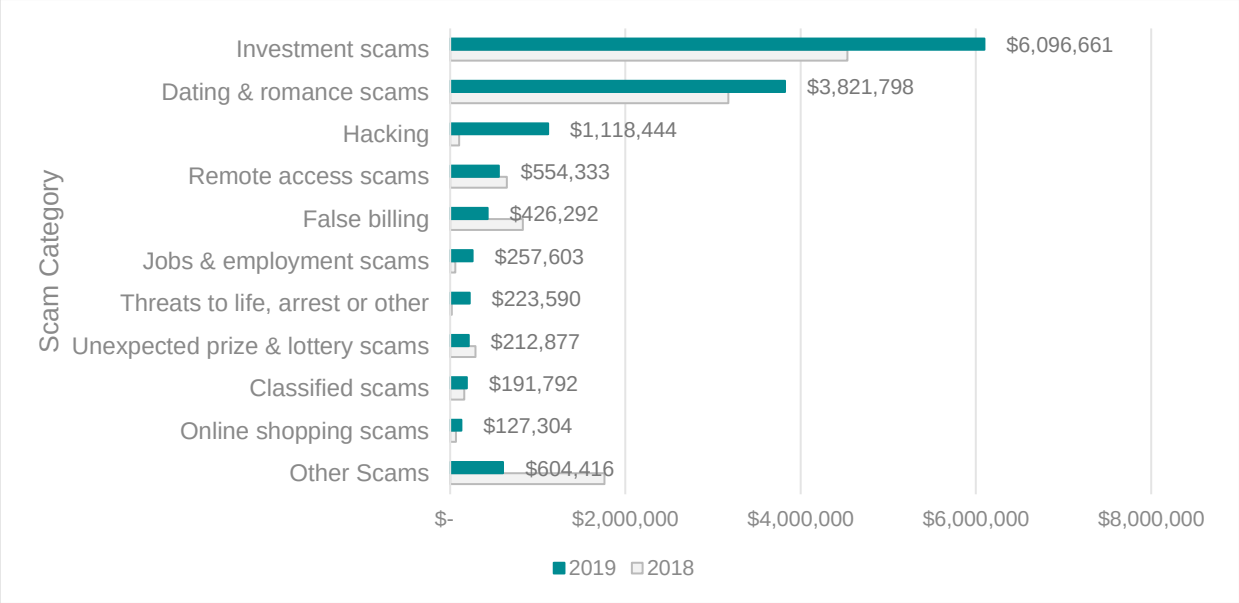
Amount lost	Number of reports	Reports with financial losses
$13,635,111 (+17%)	2,461 (+40%)	29% (-8%)

Figure 2. Total amount lost and number of reports to WA ScamNet



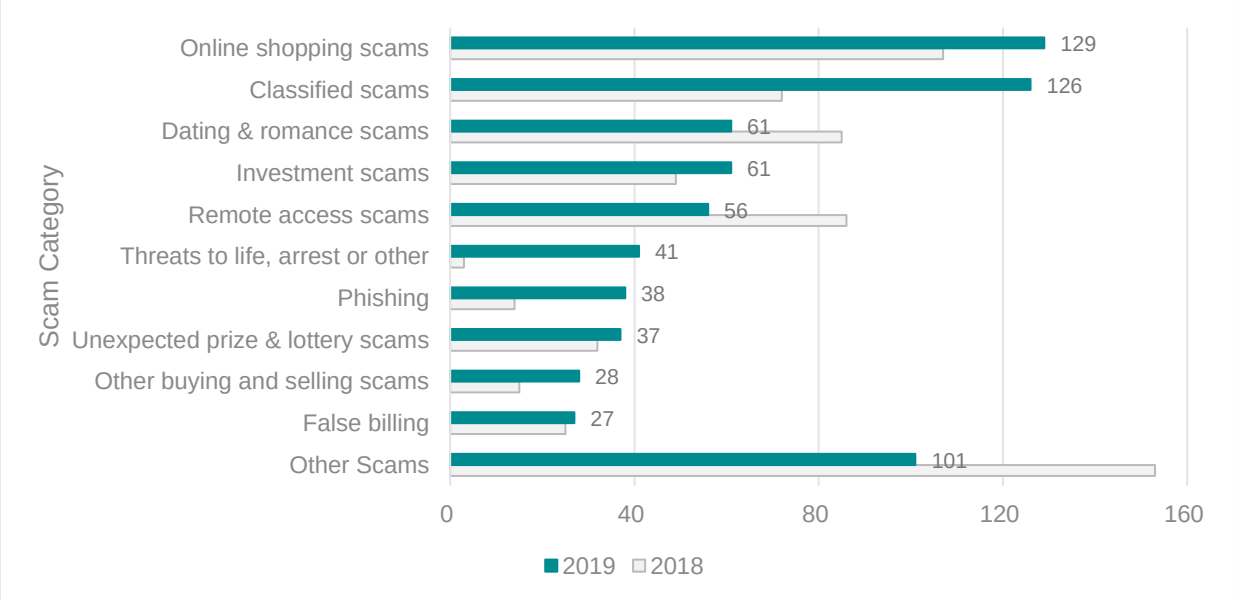
The top 10 scams, by amount lost, accounted for 96 per cent of the total losses recorded with investment scam losses contributing to 45 per cent of losses (Figure 3). The scam categories The “Other Scams” category consists of those scams that are not in the top 10 categories.

Figure 3. Top 10 scams reported to WA ScamNet for 2019 by amount lost



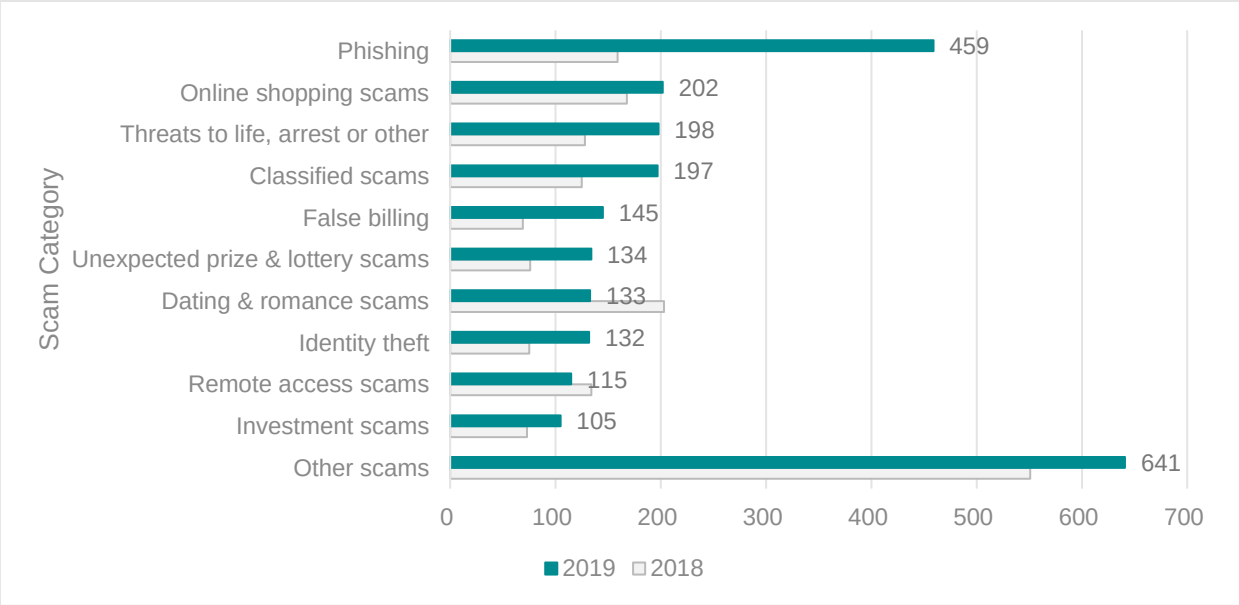
In 2019, 705 victims reported losing money to a scam with 18 per cent falling for an online shopping scam (Figure 4). The top 10 scams, by number of victims, account for 86 per cent of victims.

Figure 4. Top 10 scams by number of victims for 2019



Phishing scams accounted for 19 per cent of the total scam reports in 2019 (Figure 5) with the top 10 reported scams making up 74 per cent of the total reports.

Figure 5. Top 10 scams reported to WA ScamNet by total reports

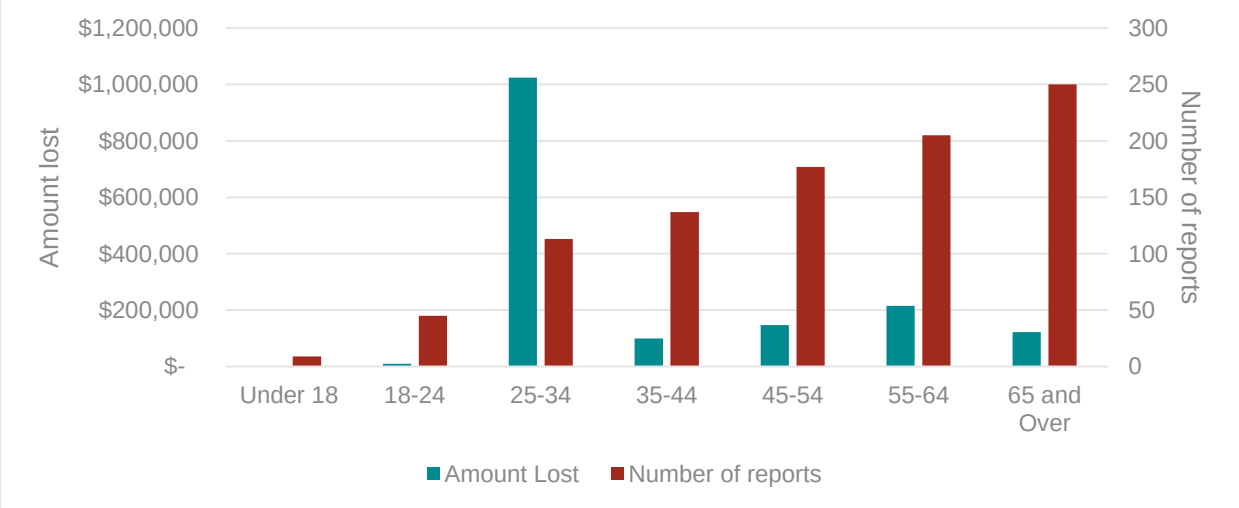


The OSR accounted for 13 per cent of the reported amount lost and 54 per cent of reports received by WA ScamNet in 2019.

Demographics

Age group information was available for 936 reports (71 per cent of total reports received through the OSR). The 25-34 year old age group reported the highest losses (Figure 6) with a total loss of $1,024,415 (61 per cent of losses with demographic information). This was due to a group of seven Australians with a combined loss of over $800,000.

Figure 6. Amount lost and number of reports by age group where reported (OSR)



While females accounted for a higher proportion of the reports made (Figure 7), males accounted for the majority of the money lost to scammers (Figure 8) in 2019.

Figure 7. Gender by number of reports

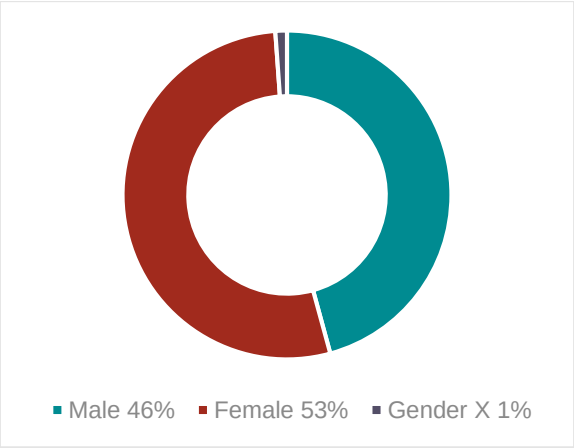
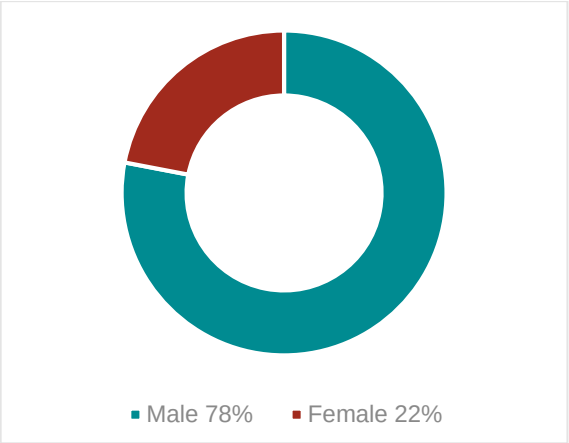


Figure 8. Gender by amount lost



Real life example: Payment redirection scam

The Yangebup Progress Association (YPA) held a Carols by Candlelight event in Yangebup which dealt with suppliers who provided services and products for the event. They received emails which contained invoices for these services/products which the YPA went ahead and paid. The YPA didn't notice anything was awry until a supplier contacted them to query where their payment was. It was at this stage they realised something was wrong and some type of hacking may have taken place.

YPA asked the suppliers to confirm their banking details, which they did. The banking information on the invoices had been changed and had not gone to the correct businesses. The total amount sent to the three suppliers was $6,569.

How the scam worked and the assistance provided by WA ScamNet:

WA ScamNet contacted YPA and discussed how this may have been orchestrated and determined the "rules" in the YPA email account had been changed.

The victim checked the rules and noted emails received containing keywords like "invoice", "payment", "bank", "bsb", "balance" and certain email accounts, would be re-directed a folder within the account (which the victim didn't notice) and once they were read the emails were forwarded to an unknown Gmail account.

The two bank accounts used as part of the scam were reported to the relevant banking institutions who in turn notified WA ScamNet the accounts were being investigated.

A post was put on the Consumer Protection Facebook page outlining how the scam worked and outlining tips for consumers to follow when paying invoices received via email and the Commissioner for Consumer Protection talked about the scam on ABC radio as part of the weekly Consumer Protection segment

After hearing about the scam online, wanting to assist, Cockburn Cement kindly donated funds to cover the cost of what was taken.

More information on how this scam works can be found on WA ScamNet's website.