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

CONSUMER PROTECTION
WESTERN AUSTRALIA

WAScamNet

Year in Review 2020

Overview

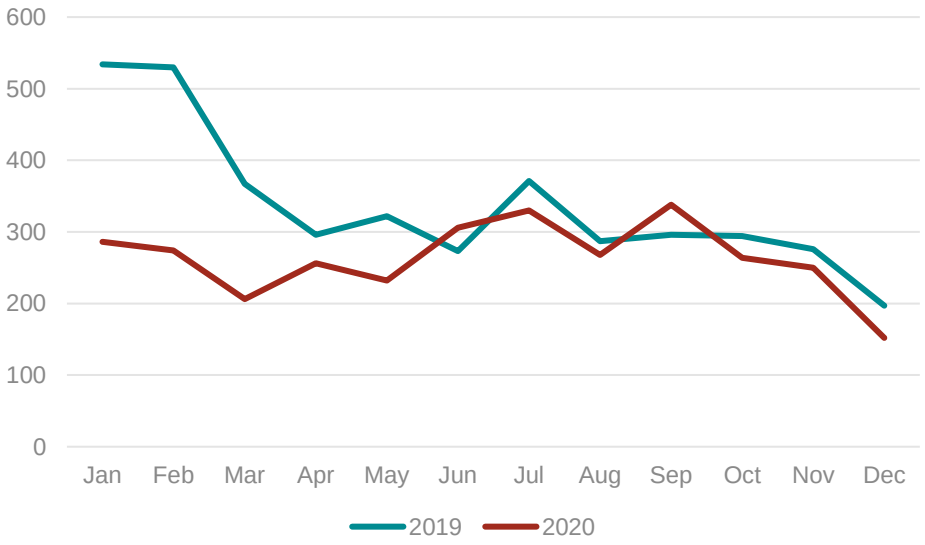
Each year, the Department of Mines, Industry Regulation and Safety – Consumer Protection Division (Consumer Protection) receives a large number of enquiries concerning scam-related problems. Many of these enquiries are lower level enquiries where consumers wish to advise Consumer Protection of an email, 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 2020, Consumer Protection's Contact Centre received 3162 calls relating to scams, 22 per cent fewer than in 2019 continuing a downward trend from 2018. The average number of calls each month was also down from 337 to 264 calls a month.

Figure 1. Scam reports received by the Contact Centre



The top two scams reported to the Contact Centre were the Australian Tax Office scam (108 enquiries, 68 per cent decrease from 2019) and the accident compensation scam (108 enquiries, 48 per cent decrease from 2019). Scams relating to Amazon increased 364 per cent from 14 enquiries in 2019 to 65 in 2020. In most cases, the scammers attempted to gain access to consumers' banking details by claiming that there was an unsolicited purchase made on their Amazon account. This increase is partially due to the COVID-19 pandemic and scammers taking advantage of consumers relying heavily on online shopping to procure goods.

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, also 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 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.

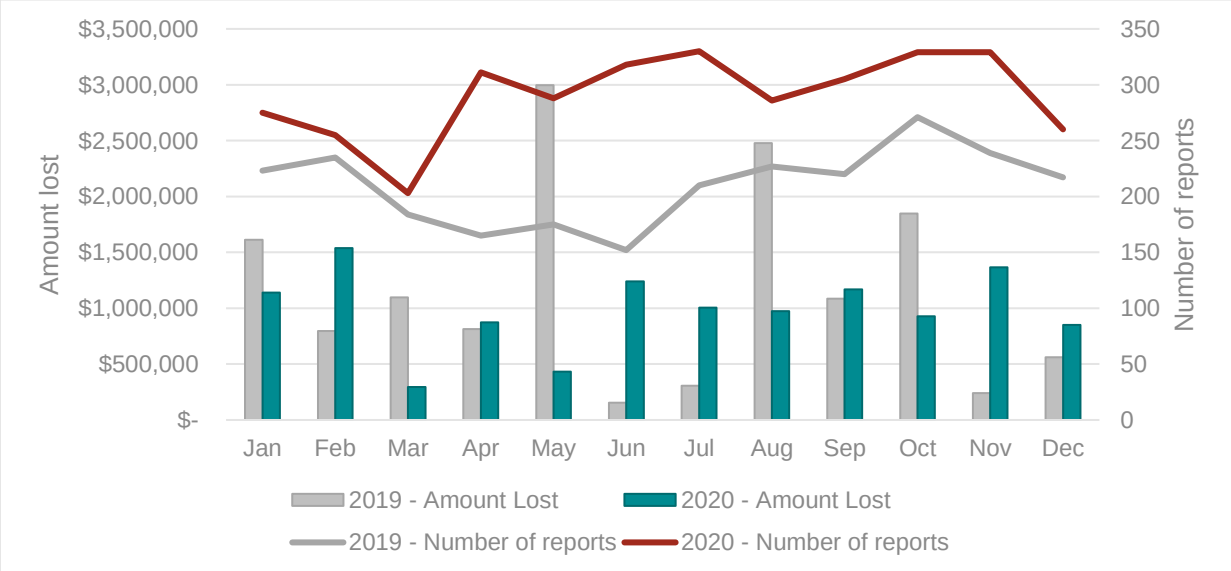
Losses

Table 1 shows the number of reports, and amounts lost, in 2020. This included two reported losses of over $900,000 both lost to investment scams in February and November.

Table 1. Statistics for reports to WA ScamNet for 2020

Amount lost	Number of reports	Reports with financial losses
$11,812,023 (-16%[1])	3489 (+39%)	952 (25%)

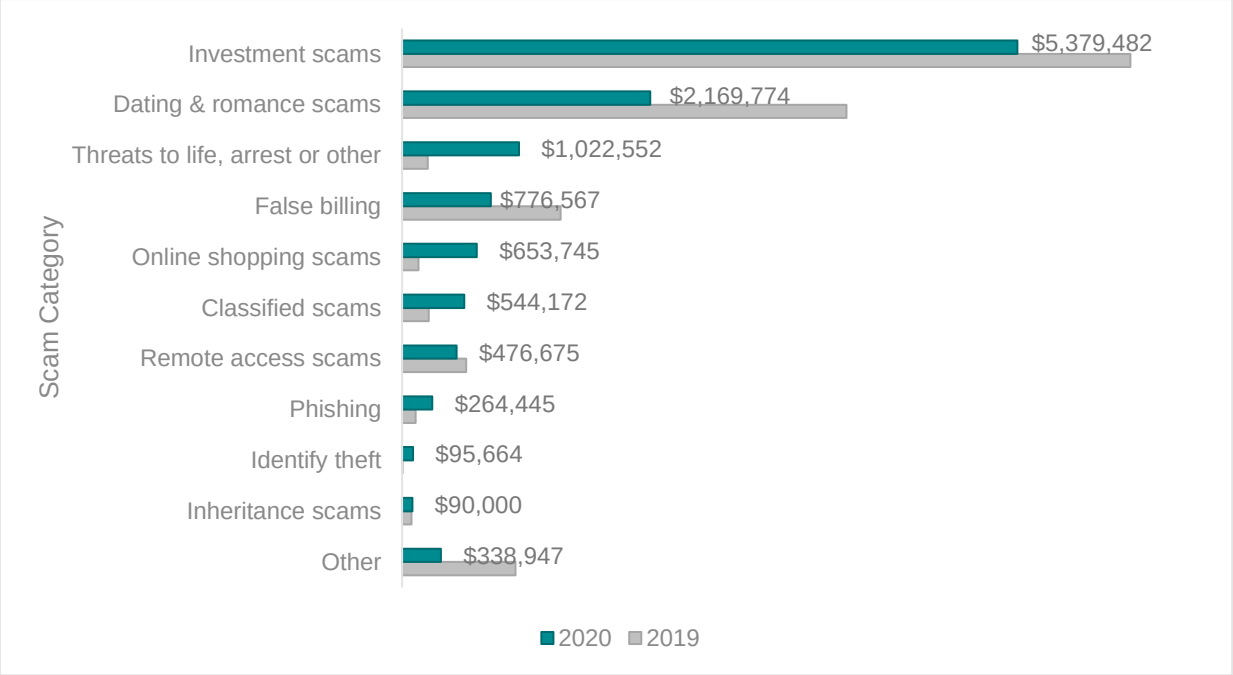
Figure 2. Total amount lost and number of reports to WA ScamNet



[1] As new information comes to light the database is updated. As such, the figures for 2019 for this report may differ from the 2019 WA ScamNet Year in Review.

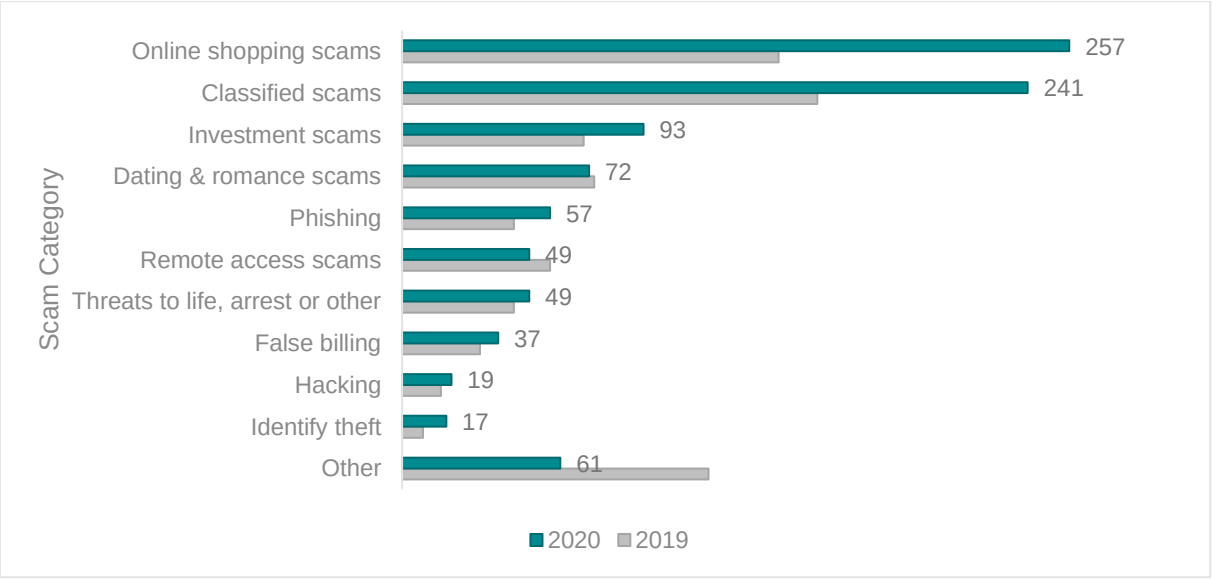
The top 10 scams, by amount lost, accounted for 97 per cent of the total losses recorded with investment scam losses contributing to 46 per cent of losses (Figure 3). The scam categories The “Other Scams” category consists of those scams that are not in the top 10 categories.

Figure 3. Top 10 scams reported to WA ScamNet for 2020 by amount lost



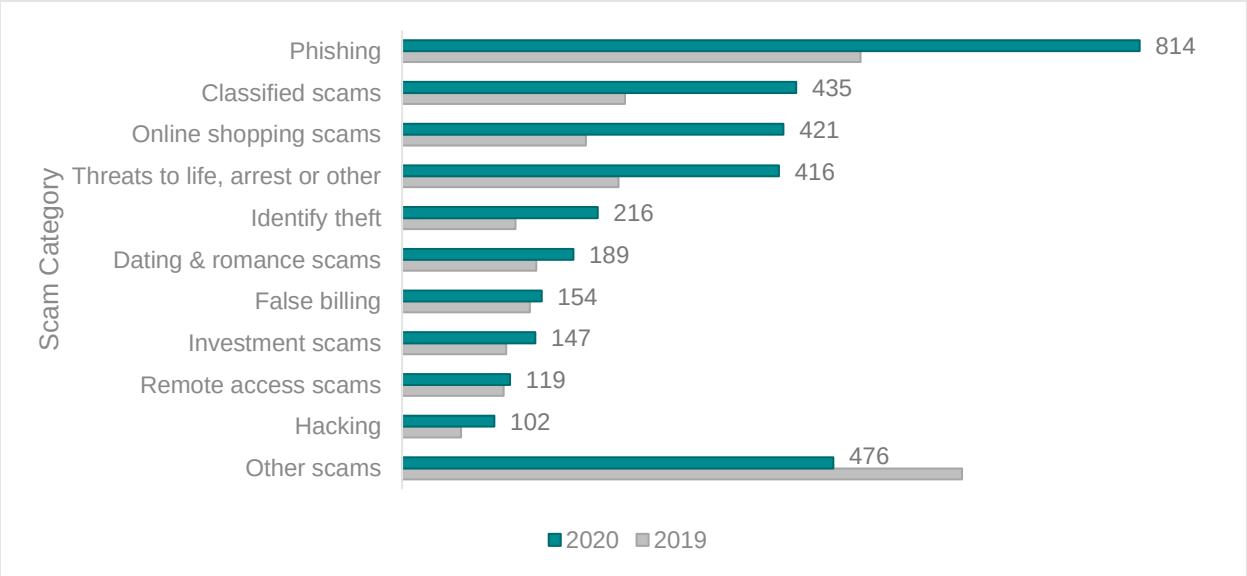
In 2020, 952 victims reported losing money to a scam with 27 per cent falling for an online shopping scam (Figure 4). The top 10 scams, by number of victims, account for 94 per cent of victims.

Figure 4. Top 10 scams by number of victims for 2020



Phishing scams accounted for 23 per cent of the total scam reports in 2020 (Figure 5) with the top 10 reported scams making up 86 per cent of the total reports.

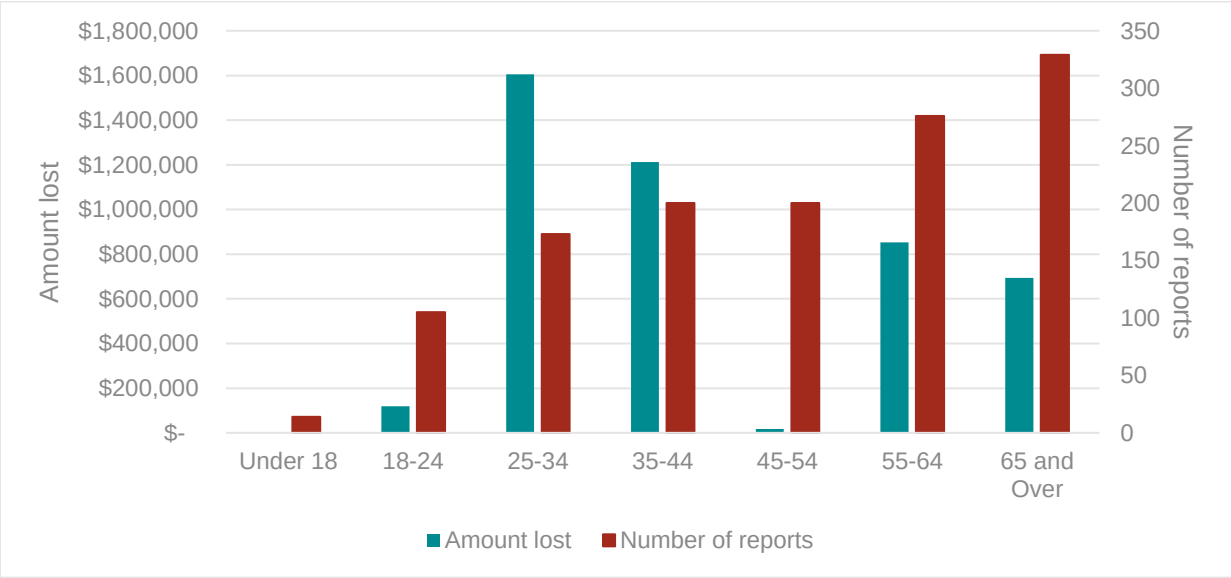
Figure 5. Top 10 scams reported to WA ScamNet by total reports



Demographics

Age group information is only captured through the OSR and was available for 1297 reports in 2020 (70 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 $1,604,728 (36 per cent of losses with demographic information). This was due to two victims with a combined loss of over $1.2 million to a dating scam and an investment scam.

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

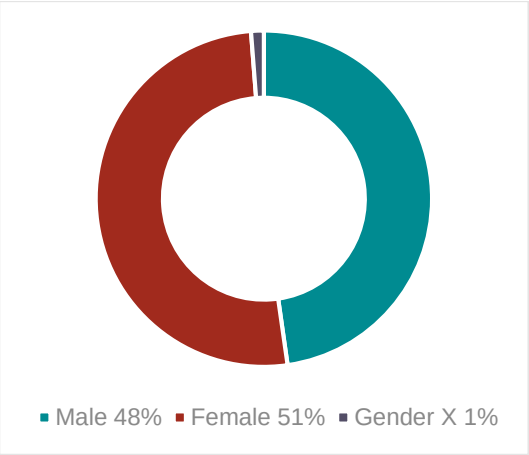
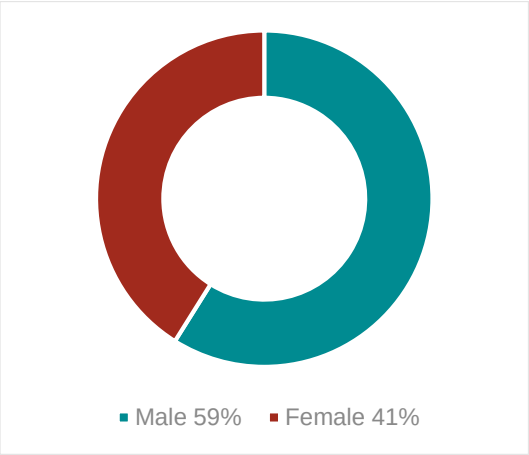


Figure 8. Gender by amount lost



Case Studies

Real life example: Online loan scam (Low Rate Finance and Mortgage King)

Victims were unable to specifically identify how the scammers were able to contact them, but they have mentioned previously searching online for personal loans and providing contact details on numerous websites. They then received unsolicited calls or emails claiming to be from 'Low Rate Finance' or 'Mortgage King' and offered a personal loan. Victims were usually people who are either not eligible to obtain a loan through big financial firms or had bad credit ratings.

Further contact with the scammers was primarily through Gmail accounts. On occasion, the scammers contacted the victim by phone or chatted through WhatsApp.

The victims were asked to make payments upfront for fees and insurance prior to receiving the funds. The victims made the payments via bank transfer but never received the loans. A request for payment of insurance upfront for a personal loan, is not usual practice.

The victims were provided an invoice and a contract that outlined what they were supposed to be getting and also stated the ABN information and the credit licence number.

WA ScamNet is aware of $82,000 in losses from victims to the 'Mortgage King' loan scam alone and approximately $10,600 in losses from victims to 'Low Rate Finance'.

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

WA ScamNet contacted the actual entities of Low Rate Finance Pty Ltd and Mortgage King Pty Limited and discussed what steps they could take to notify people that they do not offer personal loans. Mortgage King cancelled their ABN and Low Rate Finance agreed to put warnings out online notifying consumers that their ABN was being used fraudulently.

All the 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 outlined tips for consumers to follow when applying for loans online.

WA ScamNet also updated our page with relevant information

Real life example: ATO scam

Victims are cold called by random numbers stating they are from the ATO. They threaten the victim with a warrant for their arrest and explain there are fraudulent activity being undertaken under their name. The victim is asked where their nearest police station is, and told that someone from the station will call them soon to discuss the issue.

The victim then receives a call from what looks like the number of their local police station. The caller represents themselves as a police officer and states they are investigating an issue with their linked bank accounts and that it appears that they are in the midst of illegal activity. The victim is told that in order to rectify this, they need to go to various retailers and purchase gift cards, which would be used to clear their name.

In one instance, a victim went to two Big W stores in the south west region to purchase Google Play cards. The first store she purchased three $200 cards (totalling $600) then the second store, five $200 cards (totalling $1000), resulting in a $1,600 loss. At the second store she was questioned as to why she was buying the cards by staff. The victim was on the phone to the scammers whilst she was buying the cards. The staff member took the phone and told the scammers to leave the victim alone. The victim left the store but then went back afterwards seeking refunds but was refused by both stores. She had not scratched/given codes to the scammers.

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

The victim reported the scam to WA ScamNet as she was distraught over the experience. WA ScamNet contacted Big W to discuss the scam and seek a remedy for the victim, given the cards had not been used. After liaising with Big W, WA ScamNet was able to obtain a full refund for the victim. It was made easier for the victim by only having to go back to one store and have the full amount refunded back to her.

The victim went back to the store and received a full refund. She was extremely grateful as she has a baby on the way and was struggling to make payments on bills.

Big W sent out information to all their stores on the process on assisting victims when they have been caught up in these scams and refunding where possible, especially when the cards had not been redeemed.

WA ScamNet also updated our page with relevant information

For 2020, there were 150 reports received in relation to the ATO Scam, 21 victims with a total loss of $251,600. WA ScamNet was able to assist in the recovery of $2715.

Social media alerts were sent out in October 2020 regarding the spoofing of Western Australia police station numbers as part of the ATO scam, and Consumer Protection shared a post from 6PR that had an attached scam call file which detailed what the scammers say when they call.

Media release was issued on 16 October 2020 warning consumers of the new scam calls going out claiming to be ATO, Department of Home Affairs and Services Australia. 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.