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

Year in Review 2022

CONSUMER PROTECTION WESTERN AUSTRALIA

WAScamNet

Overview

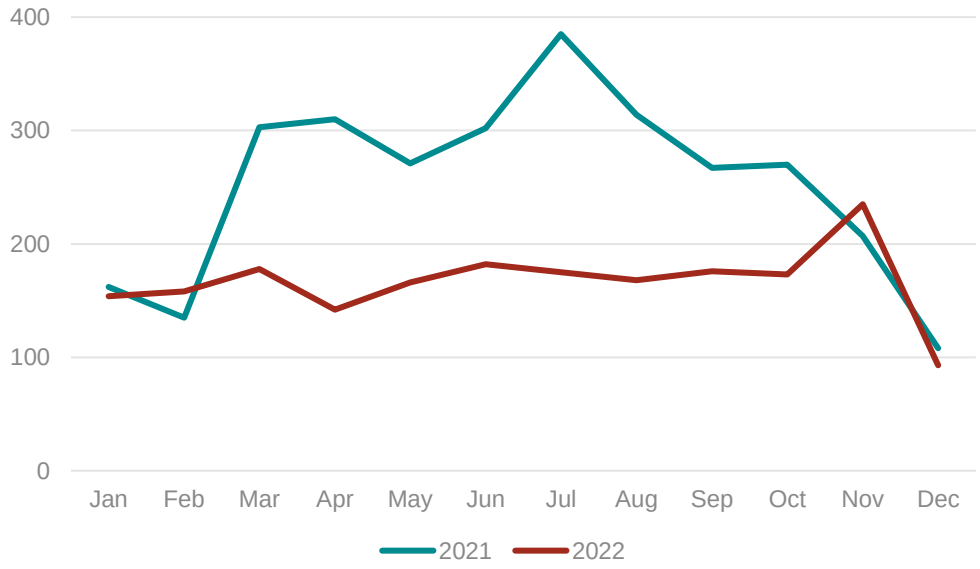
Each year, the Department of Mines, Industry Regulation and Safety – Consumer Protection Division (Consumer Protection) receives a large number of enquiries concerning scam-related problems. Many of these enquiries are lower level where consumers wish to advise Consumer Protection of an email, phone call or some form of interaction 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 Fraud Liaison Officers, WA ScamNet team. These enquiries tend to be more detailed in nature, often including situations where consumers have fallen victim to fraudulent activity, by way of a scam and lost money or personal, banking 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 Western Australia (WA) and nationally.

Contact Centre

In 2022, Consumer Protection's Contact Centre received 2,000 calls relating to scams, 34 per cent fewer than in 2021, thus continuing a downward trend from 2020. The average number of calls each month was also down from 253 to 167 calls a month.

Figure 1. Scam reports received by the Contact Centre



The top two scams reported to the Contact Centre were the Amazon phishing scam (115 enquiries, 53 per cent decrease from 2021) and the cryptocurrency investment scam (65 enquiries, four per cent decrease from 2021). Scams relating to the myGov phishing scam increased 2,650 per cent from two enquiries in 2021 to 55 in 2022. In most cases, the scammers attempted to gain access to consumers' banking details by claiming the consumers were entitled to a refund.

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, this WA ScamNet Year in Review only focuses on reports and victims in WA.

The OSR allows people to report a scam to WA ScamNet of which they have fallen victim, either anonymously, or on behalf of someone else 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 demographic information.

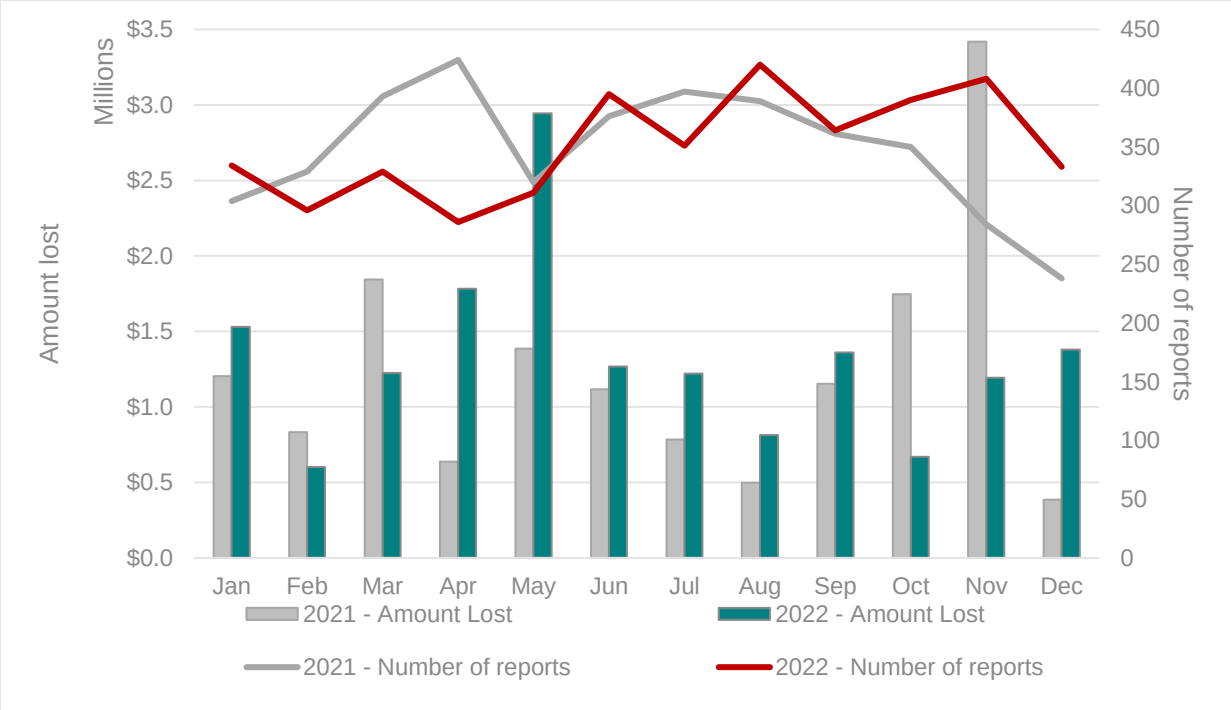
Losses

Table 1 shows the number of reports and amounts lost to scams in 2022. This included one reported loss of $800,000 in May 2022 (dating and romance scams) and one reported loss of $732,000 in April 2022 (phishing).

Table 1. Statistics for reports to WA ScamNet for 2022

Amount lost	Number of reports	Reports with financial losses
$15,988,513 (+7%[1])	4,217 (+1%)	1,203 (+15%)

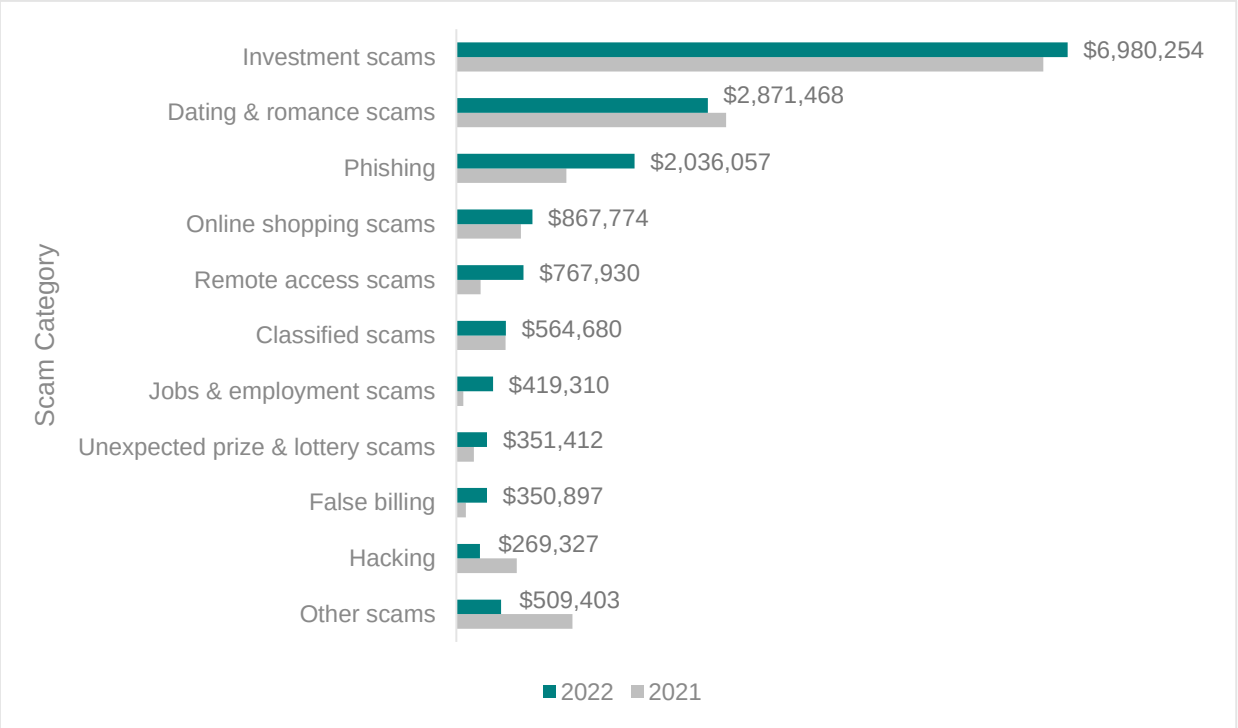
Figure 2. Total amount lost and number of reports to WA ScamNet



[1] As new information comes to light the database is updated. As such, the figures for 2021 for this report may differ from the 2021 WA ScamNet Year in Review report.

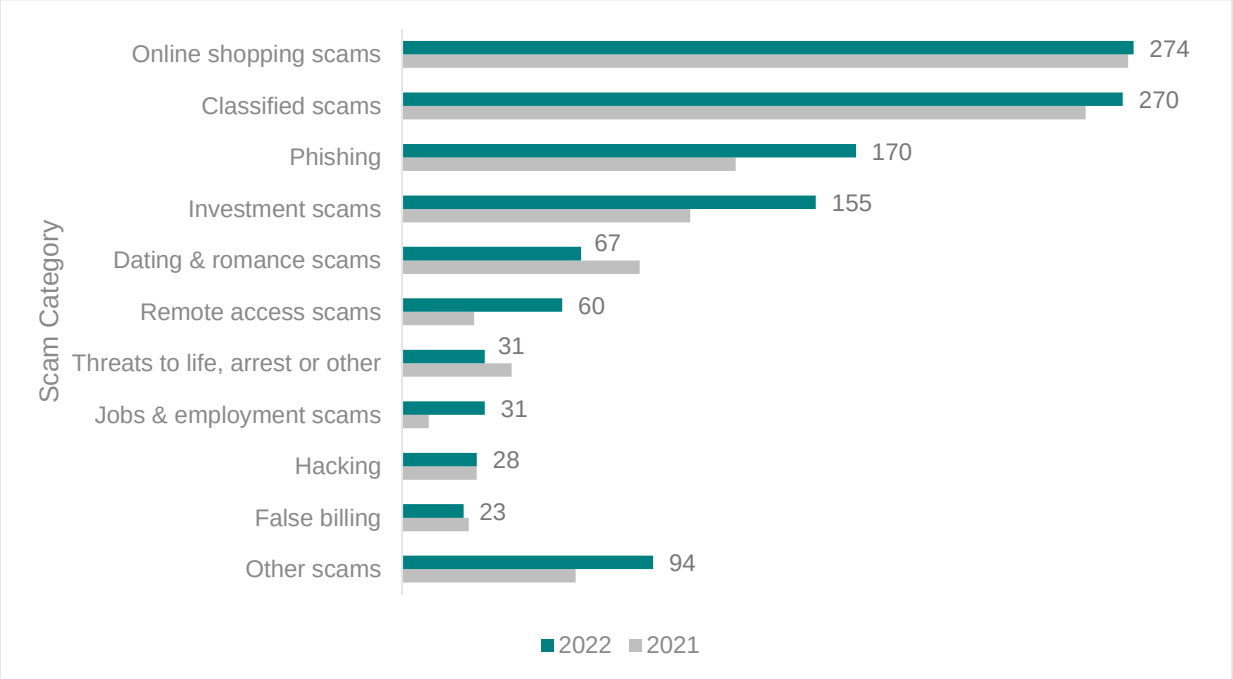
The top 10 scam categories in 2022, by amount lost, accounted for 97 per cent of the total losses recorded with investment scam losses contributing to 44 per cent of losses (Figure 3). The “Other scams” category consists of those scams that are not in the top 10 categories.

Figure 3. Top 10 scams reported to WA ScamNet for 2022 by amount lost



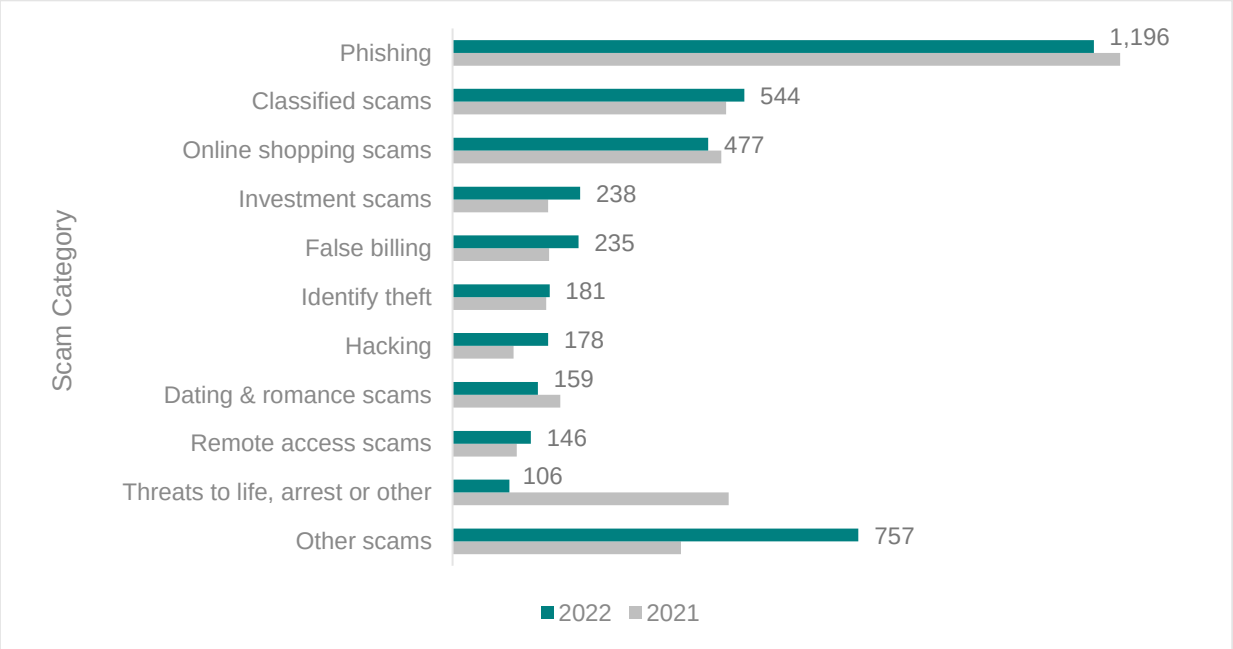
In 2022, 1,203 victims reported losing money to a scam with 23 per cent falling for an online shopping scam (Figure 4). The top 10 scams, by number of victims, account for 92 per cent of victims.

Figure 4. Top 10 scams by number of victims for 2022



Phishing scams accounted for 28 per cent of the total scam reports in 2022 (Figure 5) with the top 10 reported scams making up 82 per cent of the total reports.

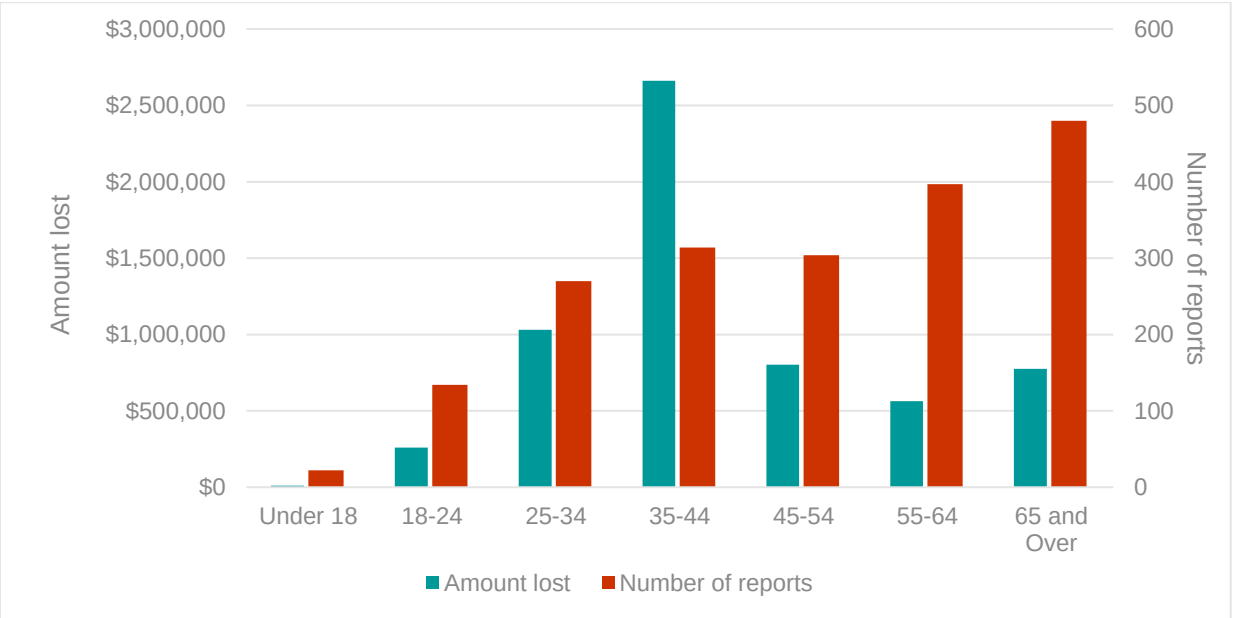
Figure 5. Top 10 scams reported to WA ScamNet for 2022 by total report



Demographics

Age group information is only captured through the OSR and was available for 1,921 reports in 2022 (76 per cent of total reports received through the OSR). The 35-44 year old age group reported the highest losses (Figure 6) with a total loss of $2,660,826 (44 per cent of losses with demographic information). This was due to two victims with a combined loss of over $1.1 million to hacking and dating and romance scams.

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



Not only did females account for a higher proportion of the reports made (Figure 7), they also accounted for the majority of the money lost to scammers (Figure 8) in 2022.

Figure 7. Gender by number of reports

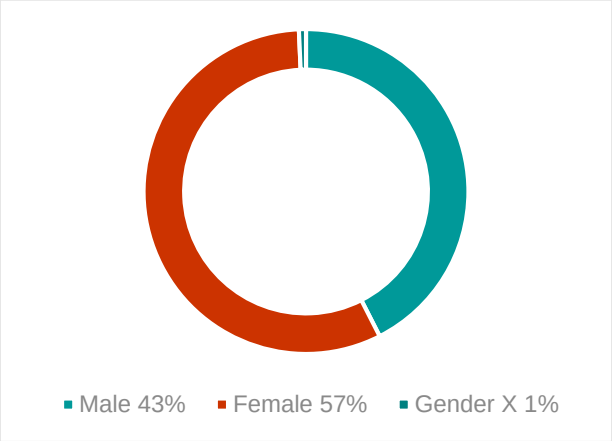
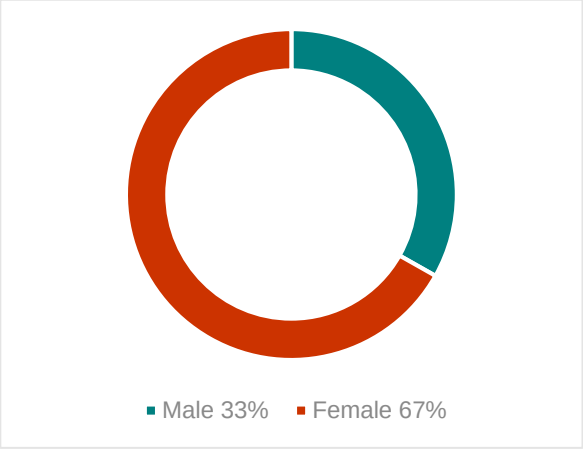


Figure 8. Gender by amount lost



Case Studies

Real life example: Investment scam – cryptocurrency

In 2022 WA ScamNet has received 73 reports (58 victims with a loss total of $4,172,852) in relation to crypto investment scams.

Report - $80,000 loss

WA ScamNet received a report that a man had fallen victim to a crypto currency Investment scam. The victim thought, he had been dealing with a legitimate company who kept advising him that they had offices in Australia.

The victim initially spoke to “Bryan”, introducing himself as his account manager and started with an introduction to crypto trading. The victim then started speaking to “Alex” who was going to keep helping him with investing and making money.

The victim was also contacted by “Julia” who alleged to be from the compliance department. She asked the victim for ID documents so that his account could be set up. These included driver’s licence, proof of address documents and proof pf payment (they requested a picture of a transaction on a bank statement that shows the transactions that were made to the company). The victim sent these documents.

The victim opened up an account on a website which appeared to be legitimate. When he logged in to the account he could see the trades he was making.

He was told he needed to keep sending money to protect his account from bankruptcy. He was told that his investment returns were high and, to keep it high, more money was needed.

The victim then saw that some of the investments would go down which would then prompt a request for him to invest more.

The victim ended up sending $80,000 (via crypto wallet) and was never able to withdraw any of the supposed profit.

The origins of the emails that were sent to the victim changed over time. They had two different websites associated with the scam that operated for a short time and is now no longer operating.

The victim was contacted nearly every day with advice on what to trade and how much to invest. The high-pressure sales techniques meant the victim would go along with what they recommended, mainly to get them off the phone.

Real life example: Attempts to gain your personal information – Hi Mum/Dad Scam

How the scam worked:

Victims respond to a SMS or WhatsApp message that starts with Hi Mum or Dad and purports to be coming from loved ones seeking urgent help with paying various bills. The messages give an excuse as to why the number being used is different to normal, such as phone is broken, battery flat, using a friend's phone etc.

The message will say they need urgent assistance and give bank details to where the money is to be transferred, or they request credit card details.

The victim usually realises it's a scam when the victim eventually contacts the loved one via their legitimate number who confirms that they had never sent the messages.

Assistance provided by WA ScamNet

- WA ScamNet reported the bank accounts used in the scam to limit the impact on consumers and assist those who had sent funds to potential obtain a refund.
- WA ScamNet reported all WhatsApp numbers that sent the messages to Meta. Meta used the information for their own investigations.
- A new page was created on WA ScamNet website detailing the scam.
- Issued a scam alert email to the WA ScamNet email subscribers.
- A media statement was issued.