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

2018 WA SCAMNET REVIEW

WA SCAMNET REVIEW

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 concerns 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 WA ScamNet team; these enquiries tend to be more detailed in nature, often including situations where consumers have fallen victim to a scam.

CONTACT CENTRE

In 2018 Consumer Protection's Contact Centre received 5,366 calls and around 17,000 emails regarding scam related matters. The top three subjects callers enquired about made up a quarter of the total calls received. These were about: false outstanding tax debts or refunds (665 calls), accident insurance (405 calls); and the threat of the National Broadband Network being cut off if victims didn't pay the scammer (403 calls).

The most enquired about scam was in relation to victims receiving calls, voicemails or emails from the Australian Tax Office (ATO). In this scam, the scammer threatens the victim into handing over money with an imminent arrest and will threaten to send the police to their home if their demands are refused. This type of scam is not isolated to the ATO and the perpetrator will claim that the victims owe money for speeding fines or unpaid bills. The perpetrators may also convince the victim that there are issues with their visa and they could face deportation. The intention of the perpetrator is to pressure people into handing over money without the victim seeking any further assistance or information.

The second most common matter presented by scam enquiries involved situations where victims are cold called by scammers pretending to be from a crash investigation company acting on behalf of an insurance company. The scammer attempts to obtain personal information such as name, date of birth, car registration, driver's licence and bank details supposedly for referral to an injury claims or compensation service promising the victim financial gain. WA ScamNet believes this is a phishing scam with the potential for identity theft if the target provides the requested information.

With the rollout of the National Broadband Network (NBN) there has been an increase in scams where a robotic voice advises victims over the phone that as the NBN is available in their area, their phone and internet will be disconnected within the next 24 hours unless connected straight away. The victim is then prompted to press 1 to be connected to a technician. The call is then transferred to a call centre where the victim has the potential to become a victim of ID theft or lose money. NBN Co has also issued a media release warning consumers not to respond or provide personal information to unsolicited callers or door knockers.

WA SCAMNET

Overview

Enquiries that Consumer Protection's Contact Centre deems to require more specialist attention, including where money has been lost, are transferred to WA ScamNet. The ScamNet team also take direct enquiries through the online scam report form and through a dedicated email address. These contacts are classified into scam types which have been set by the Australian Competition and Consumer Commission (ACCC)[1].

WA ScamNet received 1,176 contacts from Western Australians regarding losses incurred or concerns with scams in 2018, an increase of 27 per cent from 2017. Of those 1,176 contacts, 569 (48 per cent) reported losing between less than $10 through to $1.5 million. The proportion of contacts experiencing a monetary loss as compared to those who did not lose any money also increased from 43 per cent to 48 per cent in 2018.

Table 1. Scam types and number of victims

	2017	2018	Variance #	Variance %
Buying and selling	163	279	116	71%
Unexpected money	32	86	54	169%
Dating and romance	51	74	23	45%
Jobs and investment	52	57	5	10%
Attempts to gain your personal information	58	35	-23	-40%
Unexpected winnings	15	35	20	133%
Other	2	2	0	0%
Threats and extortion	23	1	-22	-96%
Fake charities	4		-4	-100%
Total	**400**	**569**	**169**	**42%**

Victims and Losses

There was a 32 per cent increase in loss amounts and an increase of 42 per cent of the number of victims who reported to WA ScamNet in 2018 from the previous year. Victims suffered combined losses of $10.7 million in 2018, compared to $8 million in 2017 (Table 2).

This year there was a significant spike in issues involving job and investment scams[2] with a 37 per cent increase of $1.2 million lost to these scams. This was due in part to a victim who had sent over $1 million. Investment schemes involve getting the victims to part with money on the promise of a questionable financial opportunity. This includes binary options trading or scammers claiming to be stock brokers or portfolio managers peddling low-risk investments with high returns.

A smaller portion of the job and investment scams category consisted of scams where the victim had been convinced they had a guaranteed way to make fast money or a high-paying job for little effort. For example, being offered a job to use your bank account to receive and pass on payments for a foreign company.

[1] https://www.scamwatch.gov.au/types-of-scams
[2] https://www.scamnet.wa.gov.au/scamnet/Scam_types-Jobs__Investment.htm

In 2019 the ACCC has re-categorised the Jobs and Investment scams in to two new categories; Investments, and Jobs and Employment. Investment scams will include betting and sports investment scams and general investment scams, and the Jobs and Employment scam category will include pyramid schemes as well as general employment scams. This will allow a clearer distinction to be made between these types of scams.

Table 2. Scam types and value of losses

	2017	2018	Variance #	Variance %
Jobs and investment	$3,290,303	$4,501,432	$1,211,129	37%
Dating and romance	$2,037,997	$2,958,633	$920,635	45%
Buying and selling	$945,676	$1,710,852	$765,176	81%
Unexpected money	$490,226	$756,297	$266,071	54%
Unexpected winnings	$101,673	$488,040	$386,367	380%
Attempts to gain your personal information	$1,041,322	$209,087	-$832,235	-80%
Other	$6,616	$56,000	$49,384	746%
Threats and extortion	$49,258	$550	-$48,708	-99%
Fake charities	$110,820		-$110,820	-100%
Grand Total	**$8,073,892**	**$10,680,891**	**$2,606,999**	**32%**

Payment Interception scams

Payment interception scams occur when a scammer posing as a legitimate supplier or contractor emails the client to say that their bank details have changed. The email is doctored to look identical to the supplier/contractor's email address and so the scam is often only detected when the legitimate business asks why they have not been paid.

Another type of this scam is when scammers pose as the CEO of a company, or another similar senior position, after copying an email account. An email is sent to a company employee asking them to transfer money to a bank account which appears to have come from the legitimate CEO. Both of these scams occur when email accounts have been compromised and hijacked.

In 2017, WA ScamNet received 20 contacts about these scams with 12 victims reporting a combined loss of $1.1 million. In 2018, the number of contacts increased to 27 contacts with 10 victims losing a combined total of $294,000.

ATO scam

The ATO scam changed in 2018 with a more aggressive scammer contacting the victim informing them that they need to contact a phone number in relation to an outstanding tax debt, or face imminent arrest and jail time. The scammer pretends to be from the ATO or the police to scare people into believing the contact is legitimate. They will then often tell the victims to buy gift cards like iTunes or Google Play to 'pay' the tax debt.

The number of reports of this type of scam increased by 36 reports to 48. Of the 48 reports, 29 victims reported losses totalling approximately $111,000 with one victim losing over $10,000. This is a significant increase from the $18,000 from five victims reported in 2017.