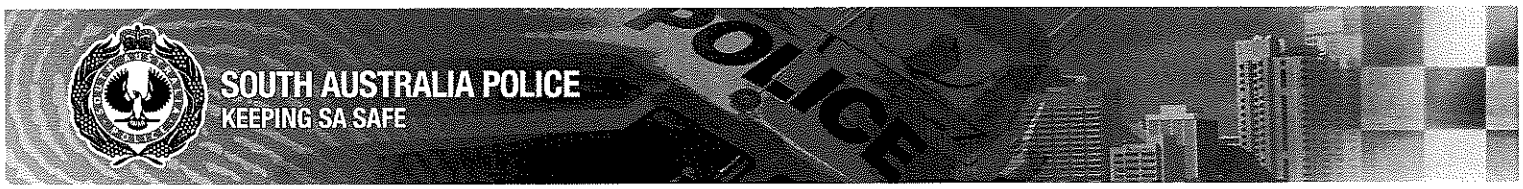


Your Ref
Our Ref
Enquiries
Telephone
Facsimile

Commemorating COMMUNITY 1838-2013 SERVING THE 175 Years
SOUTH AUSTRALIA POLICE

Mr Stephen Palethorpe
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
(inquiry into Financial Related Crime)

C/- Rosalind.McMahon@aph.gov.au
via committee's website

Dear Mr Palethorpe

Please find attached SAPOL's submission into the **Inquiry into financial related crime**.

(a) The character, prevalence and impact of financial related crime in Australia.

The impact of financial and identity related crime continues to be many and varied. Technological enhancements enable offenders to facilitate financial crimes on line and in relative anonymity rather than the traditional face-to-face meetings.

Victims range from state based, transnational and international persons as well as business entities. Perpetrators are often offshore and out of reach of Australian jurisdictions, which frustrate investigation and apprehension.

Rapid electronic technology has increased the ease of access to communications and financial institutions where monies can be transferred almost instantaneously from account to account throughout the world.

The introduction of other electronic payment types such as Bitcoin and PayPal has assisted the transfer of funds away from traditional financial reporting systems.

Identity theft (false identification) whether fake, or fraudulently obtained has become important "currency" for criminals and assists suspects to avoid detection.

Financial crime (including money laundering) and Identity theft remains particularly attractive to organised crime groups.

Rapid technological change provides an environment and opportunity for criminals to exploit inexperienced on-line users (often older persons) who are unable to keep pace with change.

The impact of crime is well illustrated in advanced fee frauds such as dating and boiler room scams (generally from high risk countries). Victims have mortgaged their houses, forwarded their life savings or borrowed monies from family and friends and even committed fraud to fund these scams. This has long and lasting ramifications for victims both emotionally and affecting their financial stability. This may have an impact on governments as these persons may require greater access to social services as a result.

(b) ***The methods and practices used by perpetrators of financial related crime (including the impact of new technologies).***

The assumption of false identities (Identity Theft) is an enabler for criminal offending such as fraud and money laundering by opening false bank accounts or fraudulently obtaining credit cards. It also assists persons to remit funds interstate and overseas quickly and with increased opportunity to avoid detection.

The use of genuine person's bank accounts ("money mules") in an effort to avoid detection of authorities is also prevalent. Often these persons are unwitting victims of scams rather than complicit in the crime.

Persons orchestrating these activities are often located overseas and there is very limited ability of the state and Commonwealth Law enforcement agencies to investigate these offenders in a timely and economic manner.

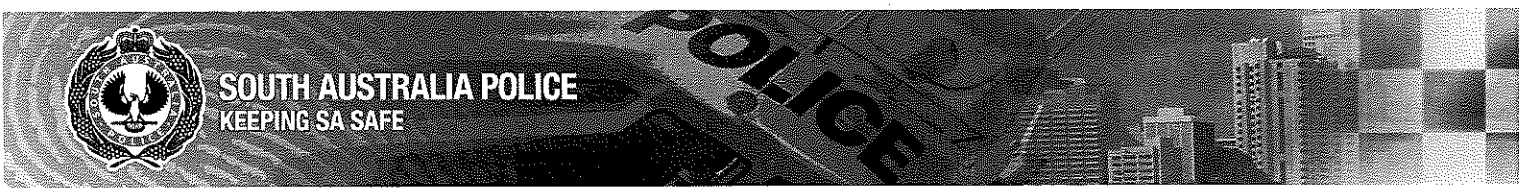
The use of VOIP telephone companies by overseas offenders to obtain local numbers to provide legitimacy to their operations has also been identified.

Software is utilised to "anonymise" or disguise the true origin of IP addresses, which frustrates law enforcement efforts to identify and locate offenders.

(c) The involvement of organised crime

The ease of access to financial services and banking systems driven by consumer forces will attract organised crime groups. Professionals such as lawyers, accountants and land conveyancers are being employed to legitimise funds being unlawfully obtained. Some examples of organised crime group's activities that have been detected include the following;

- Boiler room scams. The organised and coordinated mass targeting of "investors" from overseas has been seen in Australia where investors have forwarded thousands of dollars overseas for non-existent investments.
- Advanced fee frauds involving countries considered to be high-risk destinations. Offenders actively target dating and other online sites inducing vulnerable persons to forward significant amounts of monies under various pretexts.
- Organised syndicates involved in cannabis grow houses (often with rentals under false names) are arranged by organised groups where monies are laundered and later remitted overseas.
- On line auction frauds and website compromises stealing personal information.
- Laundering of monies through false accounts, real estate and vehicles.



(d) ***In relation to money laundering – the large number of high denomination banknotes in circulation.***

Nil submission.

(e) in relation to Identity Fraud- credit card fraud in particular

The compromise of EFTPOS terminals or skimming of credit card details, which are then, either on sold or encoded on to cards for persons to transact on purchasing desirable goods. These goods are either purchased to order or sold via on line stores and include phones, computers and tablets, cameras and other high-end goods. Syndicates are highly organised and show a degree of sophistication in respect to skimming of data and the coordination of spending.

The use of prepaid credit and store cards used to encode skimmed credit card data. These cards are transacted on at various merchants either for personal use or on sold for profit. They are also used to launder money.

ATMs being compromised (skimmed) where card details and passwords are collected and later transacted on.

A significant amount of skimmed data can be electronically transferred instantaneously to outside jurisdictions where they are on sold or transacted on. The volume of offending can take many months to investigate.

The combined use of traditional forgery methods utilising new electronic technology leading to an ability to commit high volume offending continues to occur.

Commonwealth legislation has minimal impact on credit card fraud as most credit card fraud offences are investigated by state law enforcement agencies investigating state based offences.

(f) the operation and effectiveness of Commonwealth legislation, administrative arrangements and law enforcement strategies

Nil submission.

(g) the role of the Australian Crime Commission and the Australian Federal Police in detecting financial related crime

South Australia Police have been involved in conjunction with the Australian Crime Commission on a case by case basis in respect to the involvement of organised crime with a financial flavour.

There is on-going contact with the Australian Federal Police in respect to the identification of counterfeit notes and importation of border controlled drugs.

(h) the interaction of Commonwealth, state and territory legislation and law enforcement activity

Joint investigations should be encouraged and not hindered by impediments to information exchange.

SAPOL (CECB) have been involved in joint investigations with the Australian Crime Commission and often work closely with the Australian Securities and Investments Commission (ASIC).

Due to different focuses -there is unlikely to be a joint agency commitment between the AFP and state agencies.

(i) the extent and effectiveness of relevant international agreements and arrangements

Mutual Assistance requests are cumbersome and time consuming. The cost of translating material from non-English speaking background can also be prohibitive. The delay in the provision of requested material can often frustrate investigations and the court process.

Assistance in foreign jurisdictions (dependent on Country) is often not pursued due to the convoluted process and uncertainty of results.

(j) the need for any legislative reform

Bankers Orders

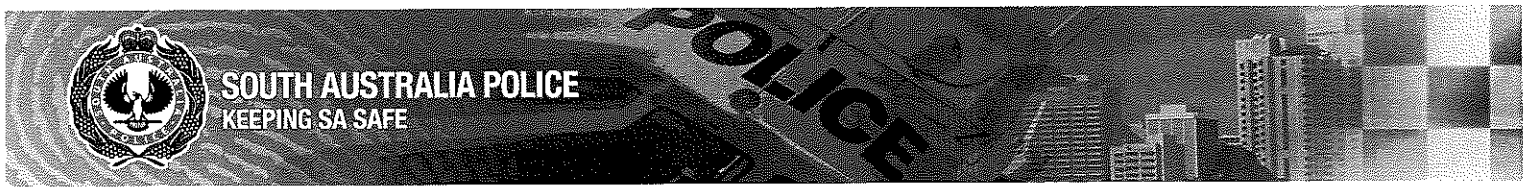
- Substantial delays are experienced when requesting information from financial institutions served with banker's orders- including follow up requests for additional information and supporting affidavits.
- Receiving banking information in electronic format would greatly assist efficiency in investigations and financial analysis.
- Setting timeframes on financial institutions to comply with court order/warrants or bankers orders.

Simpler access to national databases (State and Commonwealth) of driver's licences, passports and other forms of photographic identification would enhance identity theft and other related investigations.

A national roll out of facial recognition technology across all government agencies would assist in the timely identification of suspects.

Given the advance in technology the timely exchange of information between government and non-government agencies should be streamlined and made clearer for law enforcement purposes and for the subsequent use of information in court.

The ability to conduct the real time stopping of transfers or access to accounts. Often where a fraud is reported or suspicious activity is identified on an account is made, there is a delay in freezing the accounts- particularly where the consent of the account holder is not available.



Identity Theft Certificates
Consideration for a National Victim's of Crime Certificate- recognisable throughout Australia by Government and non-government agencies including financial institutions and credit reporting agencies where a person has had their identity compromised.

In South Australia a court upon conviction issues an ID Theft Certificate. Often cases can take a significant length of time to resolve- a certificate could be issued (on the balance of probabilities- similar to a restraint order) where a victim has reported a crime to police. The victim may then be able to use the recognised certificate to commence the process of restoring their identity.

Little if any use of Commonwealth law enforcement legislation is made or relied upon by state based agencies in the policing of serious and organised financial related crime unless the investigation is conducted under the auspices of a joint agency taskforce arrangement. Often there are practical issues between State and Commonwealth based legislation (and authorities) and subsequent prosecutions.

(k) any related matters

Unexplained Wealth investigations (UEW) are complex and protracted investigations that traditionally target organised crime entities that hide assets to avoid asset confiscation and taxation enforcement.

Disclosure of information held by State and Commonwealth government agencies to identify possible targets, make a preliminary assessment, identify, locate and trace wealth or otherwise assist an investigation and proceedings is essential.

Many Commonwealth agencies are governed by specific legislation, which regulates the collection and subsequent disclosure of information. In almost all cases disclosure of information is prohibited by statutory provisions, which contain specific exceptions permitting disclosure. In the absence of such provisions, the disclosure of information is governed by the Australian Privacy Principles (Cth). This Act also governs the release of information by non-government organisations with an annual turnover of more than $3 million.

A number of statutory or other prohibitions prevent the voluntary disclosure of information held by key Commonwealth government agencies including Centrelink, Department of Immigration and Citizenship, Australia Post and the Civil Aviation Safety Authority.

Similarly, information lawfully obtained from telephone interception cannot be disclosed for unexplained wealth purposes. Additionally, whilst there is scope under the *Australian Crime Commission Act 2002* to disclose information for the purposes of the UEW investigations, there are limitations. Disclosure of information compulsorily acquired during a coercive hearing is subject to a direction of an examiner restricting publication. Also, amendment to the Regulations would be necessary to permit disclosure of information obtained during a coercive hearing where the examinee claims the privilege against self-incrimination.

Bankruptcy - after bankruptcy the person is discharged from all provable debts. However there are some debts that are not covered by bankruptcy, including fines for breaches of law, debts arising from fraud, maintenance payments and child support. 'Fines for breaches of law' is listed as an exemption within the *Bankruptcy Act 1966* (Bankruptcy Act) but only relates to fines derived from the conviction of offences. UEW Orders are not made in respect to an offence having been committed.

Although disposing or transferring property prior to bankruptcy with the intent to defeat creditors is an offence under the Bankruptcy Act, information obtained identified that this ploy is known to be used and can make it significantly more difficult to identify assets.

Experienced administrators have identified that would be inevitable that people would petition for bankruptcy as a deliberate tactic to avoid court orders pertaining to UEW legislation.

Yours sincerely

(Gary T Burns)
COMMISSIONER OF POLICE

May 2014