



Northern Territory
Police Force

Inquiry Submission

SUBMISSION TO AUSTRALIAN JOINT PARLIAMENTARY COMMITTEE ON LAW ENFORCEMENT

Inquiry into the capability of law enforcement to respond to money laundering and financial crime.

Thank you for your correspondence of 20 June 2024 regarding the Inquiry and the opportunity to make a submission on behalf of the Northern Territory Police Force (NT Police Force).

a. The scale and forms of money laundering and financial crime in Australia, including their effect on the community and economy, the types of criminal activities they fund, the methods employed by serious and organised crime, and emerging trends and threats;

Money laundering and financial crime in the NT presents significant challenges for law enforcement. Geographically, the NT's vast, sparsely populated coastline and large number of unmonitored airstrips create an environment that allows opportunities for the smuggling of large amounts of cash, as well as drug and people smuggling. Whilst the efforts undertaken by multiple Commonwealth agencies under Op RESOLUTE are acknowledged, the environment makes detection of these kinds of offending particularly challenging. The NT is seeing the following emerging trends and threats:

- Crime related to the sale of illicit tobacco and nicotine vapes and associated money laundering is an emerging trend in the NT. This organised crime is low risk with very high rewards. There is potential risk to the community through associated violence that is occurring in Victoria that is related to Middle Eastern organised crime groups and Outlaw Motorcycle Gangs (OMCG). The money generated from these sales in the NT is used for personal enrichment by purchasing higher end real estate, as well as the transfer of significant amounts of cash overseas to the Middle East.
- Drug-related money laundering continues, through cash generated from illicit drug sales being used to make everyday purchases such as paying school fees, payment of bonds and rent, purchase of luxury goods (clothes, shoes, jewellery, watches, handbags, etc), purchase of real estate in other people's names, purchase of vehicles in other people's names or trusts, purchasing of business seats on flights and having those refunded back into bank accounts. The dark web facilitates the purchase of drugs online utilising cryptocurrency, which is difficult to trace. Casino and online gambling accounts are utilised to launder significant sums of money. Large sums of cash are being smuggled across borders by air, road, and sea.
- The under-invoicing or over-invoicing for goods and services, or multiple invoicing for goods and services (trade based money laundering) appears common. Particularly in the building trade, the exchanging of drugs with a third-party business who then organises for supply of goods, building materials, etc and issues invoices.
- Establishing cash-based businesses and shell companies to launder money, for example by commingling illicit funds with the cash flows, or paying a spouse/partner, relative or associate a "salary" from a shell company.
- Use of multiple trusts to obscure ownership of bank accounts, real property, and vehicles.
- Structuring of bank deposits to avoid threshold transaction reporting by conducting multiple branch or ATM deposits below the threshold transaction reporting limit.

NT POLICE SUBMISSION - INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO MONEY LAUNDERING AND FINANCIAL CRIME.

- Moving money through multiple accounts and different bank accounts, including the use of money remitters. Using multiple money remitters, using very small money remitters, using family members to deposit the money to the remitter, using variations in spelling of names/addresses/phone numbers which makes it more difficult to link the transaction to the offender and difficult for law enforcement to determine the ultimate recipient of funds.
- Cyber enabled financial crime and scams. In the NT, businesses have been regularly targeted through Business Email Compromise (BEC) and resultant payment redirection scams. Payment redirection scams have caused losses to businesses and individuals in the NT ranging from tens to hundreds of thousands of dollars. The largest financial harm to individuals in the NT is currently being caused by online cryptocurrency investment scams. The majority of cybercrime reports referred to NT Police involve some element of money laundering to aid the successful commission of the predicate offence.
- Money Mules – often utilised to assist movement of funds offshore. The most commonly seen methods for gaining control of an individual's bank account in cyber-related Money Laundering, are:
 - Online employment scams
 - Social engineering scams, such as relationship scams
 - Exploitation of vulnerable persons, such as residents in remote communities or international students being recruited as money mules (knowingly, unwittingly or coerced)
 - Identity theft – accounts opened using stolen credentials.

b. Australia's anti-money laundering and counter-terrorism financing (AML/CTF) legislation as well as comparison with other jurisdictions and the international standards set by the Financial Action Task Force;

The NT Police Force has no comment on this topic.

c. Proposed 'tranche two' reforms to extend the existing AML/CTF legislation to services provided by lawyers, accountants, trust and company service providers, real estate agents and dealers in precious metals and stones and implications for law enforcement;

The NT Police Force has no comment on this topic.

d. Whether existing criminal offences and law enforcement powers and capabilities are appropriate to counter money laundering, including challenges and opportunities for law enforcement, such as those relating to emerging technologies;

The NT Police Force maintains a Major Fraud Unit staffed by one Sergeant and four Constables, and an Assets Forfeiture Unit staffed by one Sergeant, two Constables and two accountants. This provides a limited capability for NT Police to investigate and prosecute financial crime and pursue the forfeiture of assets derived from or utilised in criminal activity utilising powers provided by the Criminal Property Forfeiture Act 2002 (NT) (CPFA), noting there are no resources devoted specifically to detecting money laundering.

There is real difficulty in getting bank information in a timely manner to allow analysis/seizure/restraint of property. The number of financial institutions means that only a small number of providers can be

NT POLICE SUBMISSION - INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO MONEY LAUNDERING AND FINANCIAL CRIME.

targeted as police lack sufficient resources to request and manage information to over 80 different deposit taking institutions and numerous other financial companies. Software payment platforms and payment functionality businesses make requests to get financial information more difficult.

The lack of physical bank branches in the NT adds a layer of complexity, as search warrants must be served in person. There is no mechanism for Extra-Territorial warrants to include CPFA matters, therefore a predicate criminal offence is necessary (or a production order, which has not been used). There is also difficulty in speaking with an actual person to escalate requests for financial information or get an update as to a likely response time. Police resources are frequently tied up sitting on hold to various financial institutions' phone lines, often for an hour or more. Questions/queries sent via email often experience a lengthy delay in response or are ignored. There is no after-hours support so that if a restraining order is issued by the Court near close of business the bank will not freeze the account until the next business day.

The vast majority of financial records are now digital. Current NT legislation is not fit for purpose in the areas of searching and seizing digital evidence and devices. There is currently no policy, procedure, or requisite legislation for the seizure of cryptocurrency in the NT. Law enforcement is further impeded by the absence of lawful accessibility to password protected, encrypted communications and devices. It would be welcomed if further consideration be given to ensuring law enforcement can meet community expectations in managing offending that is empowered through the use of such communication platforms and devices. Current technology allows much of this offending to occur across state and national borders. National uniform legislation would strengthen interoperability and partnerships between jurisdictions, nations, and industry.

e. The effectiveness of collaboration, coordination and information sharing between Commonwealth agencies, including law enforcement, and with authorities in other jurisdictions and the private sector;

International, federal, and jurisdictional coordination of law enforcement mechanisms to investigate money laundering and financial crime and share information related to emerging threats is coordinated by the Australian Federal Police (AFP) via Taskforce Kubera and the Operation Themis Joint Management Group, which meets quarterly and is a forum to share information and investigative techniques.

f. The role and response of businesses and other private sector organisations, including their level of awareness, assistance to law enforcement, and initiatives to counter this crime;

The Economic Crime Forum meets quarterly in conjunction with Op Themis and provides an opportunity for law enforcement and other government agencies to meet with representatives from Australia's major financial institutions to foster interagency collaboration and jointly explore opportunities for enhanced law enforcement intelligence and information exchange, interoperability and capability to combat serious organised financial crime threats to Australia.

g. The operation of unexplained wealth and asset recovery legislation, the Criminal Assets Confiscation Taskforce, and the Confiscated Assets Account;

Unexplained wealth and asset recovery legislation in the NT is contained in the Criminal Property Forfeiture Act 2002 (NT). This legislation is particularly focussed on drug related offending although the Act has a much wider application. There has been a reluctance by the DPP to use unexplained wealth legislation unless a link to criminal offending has been identified, despite none being required the Act.

NT POLICE SUBMISSION - INQUIRY INTO THE CAPABILITY OF LAW ENFORCEMENT TO RESPOND TO MONEY LAUNDERING AND FINANCIAL CRIME.

Production orders, examination orders and monitoring order powers under the Criminal Property Forfeiture Act 2002 have never been used. The difficulty in using these powers is that applications must be made to the Supreme Court and supported by affidavit. This is a time consuming process. It also means the powers are likely to never be used in relation to Local Court proceedings. The uncertainty around the operation of the powers has also meant a reluctance to use them.

h. Any related matters.

Nil.

..End..