VICTORIA POLICE

12 December 2025

Stephen Palethorpe
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600

By email only: le.committee@aph.gov.au

Dear Secretary

Inquiry into the capability of law enforcement to respond to cybercrime – Right of reply to submission

Thank you for your correspondence of 29 October 2025 inviting Victoria Police to respond to adverse comment contained in the supplementary submission of Mr Ken Gamble, Executive Chairman of IFW Global dated 3 September 2025.

Victoria Police welcomes the opportunity to formally respond to matters raised in IFW Global's supplementary submission.

As stated in our submission to this Inquiry, Victoria Police is responsible for detecting, apprehending, and disrupting offenders who commit crimes in Victoria or against Victorians. This includes cybercrimes committed against individuals, businesses and State and local governments. Combatting cybercrime is a strategic priority for Victoria Police. Cybercrimes investigated by Victoria Police include ransomware attacks, cyber-attacks, investigations into child abuse and exploitation, illicit online marketplace (darknet) investigations and cyber-enabled finance scams, the latter of which was the focus of IFW Global's supplementary submission.

While Victoria Police has a very different perspective to IFW Global on the statutory powers available to Victoria Police to respond to cryptocurrency offences, we are unable to disclose sensitive information regarding criminal investigations to be referred to other jurisdictions. Accordingly, Victoria Police provides the following high-level response to IFW Global's supplementary submission regarding police processes and legal mechanisms available to Victoria Police to restrain cryptocurrency.

Victoria Police's powers under legislation to seize, freeze and restrain cryptocurrency

We note IFW Global's statements that there are *"systemic gaps in state law enforcement responses to crypto-enabled fraud (Victoria and NSW), despite clear legislative powers and*

available freezing mechanisms", and "*existing legislative tools are available but remain underutilised",* and that Victoria Police is "*reluctant*" to use legislative powers available to it. To date, and since relevant reforms to the *Confiscation Act 1997* (Vic) (**Confiscation Act**) in recent years, Victoria Police has utilised legislative powers to seize cryptocurrency on a routine basis. There is no reluctance to use these powers when they are available to Victoria Police.

Legislative powers to seize a digital asset

Cryptocurrency is a "digital asset" for the purposes of the Confiscation Act**.** Legislative powers specific to the search and seizure of digital assets were introduced to the Confiscation Act via the recent *Major Crime and Community Safety Legislation Amendment Act 2022* (Vic). Relevantly, section 92A was introduced to enable Victoria Police to access and/or gain control of a digital asset under the authority of either a search warrant or section 92 of the Confiscation Act.

These powers are limited to search warrants issued under Part 11 of the Confiscation Act and are search warrants executed *on premises* in Victoria. Specifically, they empower police to take the necessary technical steps required to seize cryptocurrencies linked to devices seized at warrant premises. These legislative powers are not applicable in circumstances where a stolen digital asset cannot be connected to a device seized as a result of executing a warrant within the State of Victoria, or in circumstances where the alleged offender is unknown and offshore.

Legislative powers to freeze and restrain a digital asset after a suspect has been charged

Victoria Police routinely conducts confiscation investigations which run parallel to criminal investigations, especially in matters involving serious organised crime. Where suspects charged with serious indictable offences hold significant digital assets, Victoria Police will apply for a freezing order in the Magistrates' Court of Victoria to prevent the asset from being dissipated. Such applications are heard expediently and electronically, thereby ensuring the digital assets are quickly frozen.

Following a court making freezing orders, Victoria Police has the ability to freeze digital assets under the Confiscations Act for five business days, which may be extended upon a further court application. Preserving the digital assets in this fashion also makes them available for subsequent restraint through a restraining order.

The ability to freeze digital assets was the result of legislative reform in the *Major Crime and Community Safety Legislation Amendment Act 2022* (Vic) which extended the definition of "financial institution" within the Confiscation Act to include (at s 3(1)(da)) "a provider of a registrable digital currency exchange service within the meaning of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)". This amendment enabled the Magistrates' Court to make freezing orders in respect of an account held with a registrable digital currency exchange service.

Section 31D(1) is the primary vehicle by which cryptocurrency is frozen under the Confiscation Act. Pursuant to this sub-section, a police officer can apply for a freezing order if they believe on reasonable grounds that:

(a) the relevant account is in the name of a person, or that person has an interest in the account and
    (i) they have committed, or are about to commit a Schedule 1 offence, a Schedule 2 offence or a serious drug offence; or

(ii) they were involved in the commission, or are about to be involved in the commission of such an offence; or
(iii) they have benefited directly or indirectly, or are about to benefit directly or indirectly from the commission of a Schedule 1 offence or Schedule 2 offence; and

(b) an application for a restraining order is likely to be made in respect of property which the person-
(i) in whose name the account is held has an interest; or
(ii) who has an interest in the account in respect of which a freezing order is sought, has an interest.

Once digital assets are frozen, either the Chief Commissioner of Police or the Director of Public Prosecutions will make an application for a charge-based restraining order under section 16 of the Confiscation Act to restrain the frozen asset. The restrained asset may be forfeited to the State upon the suspect being convicted of the charge that underpinned the restraining order.

In circumstances where an asset has been transacted multiple times and the person of interest no longer holds the asset, the asset will still be tainted within the meaning of section 3 of the Confiscation Act, but may not necessarily be frozen or restrained. An innocent third-party who receives tainted cryptocurrency may file an application for exclusion against restraining order under sections 20 to 22A to guard their tainted asset from restraint: see sections 22(1)(b) and 22(1)(b). The effect of sections 20 to 22A is that, in circumstances where a digital asset has been lawfully transacted after it was unlawfully obtained, if an exclusion order application is made by a person other than the accused, the court may make an order excluding that person's interest in the tainted asset from the operation of the restraining order, if the court is satisfied that the person was not, in any way, involved in the commission of the offence, acquired the interest without knowing that the property was tainted property, and for sufficient consideration.

In practice, this means that while digital assets are easy to trace, if the digital asset has been transacted multiple times since it was unlawfully obtained, a restraining order would be inappropriate without a thorough investigation that evidences the context and details of each of the subsequent transactions.

Noting that an application for a restraining order under section 16 of the Confiscation Act is predicated on criminal charges being filed against a person, it follows that this person's digital assets will neither be seized nor frozen until the criminal investigation has sufficiently progressed. Invasive police action to freeze or restrain an asset needs to be supported by a thorough investigation that has yielded an abundance of evidence. Obtaining a freezing order prematurely runs the risk of notifying the suspect that they are under investigation, and worse, may prompt them to dissipate their remaining assets. Accordingly, freezing orders will not be sought until either criminal charges are close to being filed, or have already been filed.

Practically, there are thousands of active cryptocurrency businesses operating globally, in addition to Decentralised Autonomous Organisations, which are cryptocurrency exchanges that exist as software only without a centralised governing body. Even in circumstances where a court will make a freezing order against such an entity, there are fundamental issues pertaining to jurisdiction and sovereignty that make enforcement difficult and at times impossible. If the outcome of a thorough Victoria Police investigation shows persons of interest resident in jurisdictions outside Australia, then the formal process is to mark that investigation as complete and escalate

the matter to Interpol for assessment / action. It is not for Victoria Police to attempt to freeze a digital asset for a criminal matter beyond our jurisdiction.

Legislative powers to restrain assets by way of Unexplained Wealth Restraining Orders

As referred to above, the restraint powers under the Confiscation Act are predominantly charge-based. In circumstances where an alleged offender has not been charged (and is not expected to be charged within the next 48 hours), police may still have grounds to apply to a court to restrain an asset, by way of an unexplained wealth restraining order pursuant to Part 4A of the Confiscation Act.

An unexplained wealth restraining order is confined to circumstances where a police officer suspects on reasonable grounds that:

- a person with an interest in the property to be restrained has either engaged in serious criminal activity within Victoria, or
- acquired the property unlawfully and either the property is located in Victoria or the person who acquired the property is ordinarily a resident in Victoria, or
- a person has an interest in the property sought to be restrained has wealth that exceeds their lawfully acquired wealth.

Accordingly, a digital asset that has been transacted multiple times and since been lawfully acquired is not amenable to an unexplained wealth restraining order. Furthermore, in circumstances where both the asset and the person suspected of engaging in serious criminal activity are located outside Victoria, an unexplained wealth restraining order will not be available to Victoria Police.

Investigative methods and referrals processes

Noting the statement that "*investigative tools are available but remain underutilised*", we submit that there are highly qualified investigators (specialised detectives, forensic investigators and forensic accountants) within Victoria Police who are capable of tracing the movement of cryptocurrency with speed and efficiency. While comprehensive digital/blockchain tracing of digital assets is a single source of evidence that may reveal additional avenues of enquiry, in circumstances where a tainted digital asset has been relocated multiple times, a trace alone is insufficient evidence to substantiate intrusive police actions such as a court ordered freeze or restraint of property.

A trace report following the movement of funds on a public ledger such as a cryptocurrency blockchain does not provide any evidence of possession without corroborative evidence. Further, police intelligence suggests that it is often the case that cryptocurrency addresses provided by offenders are not controlled by offenders and can be controlled by innocent agents such as money remitters, those selling goods for cryptocurrency, or amateur cryptocurrency exchangers (a common way to earn money in developing economies). These parties often receive victim payments with no awareness of the underlying criminality.

Where a cryptocurrency blockchain trace identifies persons of interest in overseas jurisdictions, Victoria Police adhere to the formal process of referring relevant investigative files to the Australian Federal Police (**AFP**) and/or Interpol, without hesitation. There is a process for escalating or referring matters to Interpol involving notification first to the Attorney-General's office in Canberra,

to seek assistance from Interpol. This is a nationally standardised process with relevant forms, liaison offices, and is a routinely utilised system by Victoria Police. Victoria Police has a member embedded at the AFP run Joint Policing Cybercrime Coordination Centre (**JPC3**) in Sydney, and Victoria Police consistently works with the AFP on joint criminal investigations into cybercrime offences.

Victoria Police's responsibilities under the *Victims' Charter Act 2006* (Vic)

Victoria Police recognises the impact of crime on victims, including the impact on members of victims' families, witnesses and the broader community. Victoria Police recognises that all persons adversely affected by crime, regardless of whether they report the offence, should be treated with respect. Victoria Police also recognises that a victim of crime has an inherent interest in the response by the criminal justice system to that crime, giving rise to rights and entitlements set out in the *Victims' Charter Act 2006* (Vic) (**Victims' Charter**). In so doing, we hope to reduce the likelihood of secondary victimisation by the criminal justice system.

The Victims' Charter principles are applicable to Victoria Police as both an investigatory agency and as a prosecuting agency. While we cannot comment on the specifics regarding the case studies raised by IFW Global in its supplementary submission, Victoria Police is committed to adhering to the Victims' Charter principles, and encourages any person adversely affected by crime who believes that Victoria Police has not upheld the Victims' Charter principles to raise a formal complaint.

Operation Taipan seizure

In relation to IFW Global's comment that Operation Taipan demonstrates that Victoria Police has already used Tether wallet freezes to preserve digital assets linked to criminal proceeds, we submit that the cryptocurrency seized in Operation Taipan was stored on a cryptocurrency exchange with an Australian footprint that complied with local legislative instruments, and no "wallet freezes" were used by Victoria Police during this operation.