Reporting cybercrime

Context

Victoria Police is responsible for investigating cybercrime committed against members of the Victorian community, whether by those residing in Victoria or elsewhere.

ReportCyber is the national online reporting platform that allows members of the community to report suspected cybercrime. Victoria Police uses ReportCyber to help make reporting cybercrime easier for victims whilst supporting police members with the capability needed to provide a consistent service to victims of this type of crime.

Policy at a glance

This policy includes:

- broad crime types that may constitute cybercrime
- information and guidance on the use of ReportCyber, including what crimes must not be reported using this platform
- instructions regarding management of Cyber Incident Reporting System (CIRS) reports and roles and responsibilities and
- guidance on referrals to other jurisdictions.

Contents

Scope and application

These instructions apply to all police members.

Responsibilities and procedures

1. Overview

- Cybercrime refers to offending using technology. A broad range of crime types may be considered cybercrime, including crimes against the person (i.e., stalking and extortion) and crimes against property (i.e., hacking and online fraud. Refer to **VPM Fraud offences** for more information regarding online fraud).
- For law enforcement and other agencies, cybercrime has two aspects:
  - cyber dependent crime - directed at computers or other information communications technologies (ICTs) such as computer intrusions and
  - technology-enabled crime - such as online fraud, identity theft and the distribution of child exploitation material, where computers or ICTs are an integral part of an offence.

  Note: It does not include crime where the use of information technology is incidental to the commission of the offence, e.g., an offender might plan to commit a crime via mobile phone. In this instance, the mobile phone would be relied upon for its evidentiary value.
- The Cybercrime Squad conducts specialist investigations to detect, disrupt and prevent serious and organised crime involving complex technology. In addition, the Cybercrime Squad can provide specialist capabilities and advice to assist investigations with digital forensic evidence and covert online services including cryptocurrency.

2. ReportCyber

2.1 *Overview*

- ReportCyber is the national online reporting platform accessed from Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) website (www.cyber.gov.au/report). ReportCyber allows members of the public to report suspected cybercrime. The ACSC assigns reports to the appropriate jurisdiction for assessment via CIRS.
- CIRS reports are identifiable by a CIRS Report Number in the format CIRS-YEARMMDD-Report Number for that day (e.g., CIRS-2025xxxx-xxx). This reference number should be included in the LEDR Mk2/LEAP report as the originating report reference.
- In the circumstances where a CIRS report is assessed by the Cybercrime Intelligence Assessment Unit (CIAU), Cybercrime Squad and determined that, on the balance of probabilities, a crime has been committed, a crime report via LEDR Mk2 must be created and allocated to a police station for victim management and investigation.

2.2 *What can be reported on ReportCyber*

- Types of matters that can be reported via ReportCyber include:
  - job and investment scams
  - fraudulent online trading incidents (including eBay, Facebook Marketplace and Gumtree)

- romance fraud (i.e., where someone has posed as a romantic interest to gain a victim's trust and then exploit them financially)
- identity theft (i.e., where someone has used compromised identity information online)
- email compromise or
- ransomware, malware or other attacks on computer systems.

2.3 *Victims of crimes that must not be directed to ReportCyber*

- Victims reporting the following crimes must not be directed to ReportCyber and must be reported in accordance with **VPM Crime and event reporting and recording**:
  - family violence i.e., intimate or former intimate partners sharing or threatening to share intimate images or videos of a person online
  - where a nominated person of interest (POI) is a family member, intimate partner, or former intimate partner
  - breaches of court orders
  - crimes against the person
  - offences against children
  - where there is a risk of harm to a person
  - where police attendance is required
  - where there are concerns for a reporting person's safety or welfare, and
  - where a physical item, such as a bank card (used to make subsequent purchases) or a computer has been stolen.

  ReportCyber must not be used to report cybercrime against Victoria Police or Victoria Police systems. These must be reported via PBEA: IT-SECURITY INCIDENTS-MGR.

3. Management of Cyber Incident Reporting System reports

3.1 *Cybercrime Intelligence Assessment Unit responsibilities*

- The CIAU is responsible for the initial triage and management of all CIRS reports received by Victoria Police.
- The CIAU must assess and determine the CIRS report against the following criteria:
  - Not accepted: where it is determined on the balance of probabilities that a crime has not been committed. In these instances, the triage member should provide advice and/or direct the reporting person to an appropriate entity such as the eSafety Commissioner, the relevant financial institution, the social media platform, or the Australian Financial Complaints Authority or
  - Accepted: where it is determined on the balance of probabilities a crime has been committed.
- Where a report is accepted, the CIAU must generate a crime report via LEDR Mk2 from the CIRS report and assign it to the relevant police station.
- Where a report is not accepted, the CIAU should submit an Information Report (IR) for intelligence purposes where appropriate, i.e., anonymous reports where the contents may be of value to Victoria Police.

3.2 *Allocation of crime reports*

- Police members must take a crime report and conduct an investigation where an offence occurred within Victoria or if there is a real and substantial link to Victoria in accordance with s.80A, *Crimes Act 1958* (extra-territorial offences).

- Section 80A, *Crimes Act* provides that where there is a real and substantial link to Victoria in the commission of a crime, the offence can be reported, recorded on LEAP and investigated as a crime in Victoria. This link is established where:
  - a significant portion, if not all of the offending, has taken place in Victoria, and/or
  - the substantial harm or impact of the offence is experienced in Victoria by the victim (i.e., the offence was committed in another jurisdiction, but the impact of the crime was wholly or substantially to a Victorian-based victim).

Note: police members must also consider s.247I, *Crimes Act* (extra-territorial operation of offences) regarding the location (Victoria) of either the conduct constituting an offence or the computer or device used to store data or any other relevant extra-territorial provisions.

- Due to the sophistication of technology enabled crime to easily conceal the location of an offender. The police station in the response zone of the victim at the time of the offence must conduct the investigation and fulfill victim support obligations in accordance with the *Victims' Charter Act 2006*.
- Where the reporting person is from a business:
  - a national financial institution: the crime report must be allocated to the police station in the response zone of the affected customer, regardless as to whether the bank reimbursed the customer and carried the loss
  - a national retail company: the crime report must be allocated to the police station in the response zone where either the item was posted or the store where the item was collected regardless of the location of the company.

4. Management of investigations

4.1 *Supervisor responsibilities*

Following submission of a crime report via LEDR Mk2 from the CIAU, supervisors must follow the steps in the table below

Step	Action
1	On the LEDR Mk2 dashboard, select the relevant work unit area and status
2	On the Report Action select 'Authorise' (reports must not be marked 'Discard' or 'Not to be progressed') Note: where a report is identified as a duplicate on LEAP, the supervisor must mark it as Return to Member (Rework) and notify CIAU
3	Select 'Next' on the narrative screen then 'Authorise' on the Sub-Incident screen
4	On the Sub-Incident supervisor result confirmation screen select 'Unsolved'
5	On the Report Authorisation screen, select 'Authorise' (transaction to LEAP)
6	Mark the Case Progress Status 'Active'
7	Follow up actions required: select 'Yes' then later select Criminal Investigation
8	Assign to member
9	Press next and commit to LEAP Note: where Commonwealth offences are used to record incidents (such as cyber abuse and cyber bullying where someone is being bullied, harassed, or stalked online), they may not contain sufficient information to identify a state-based offence on the initial report narrative, however, these still constitute a prima facie offence. For accurate recording of crime, these offences must be committed to LEAP. Refer to **VPMG Commonwealth offence investigations** for information regarding conducting commonwealth investigations

4.2 *Police member responsibilities*

- The investigating member must:
  - contact the victim(s) and/or reporting person(s) and obtain further information
  - perform any further assessment, action, or investigation in accordance with **VPM Crime attendance – initial action** and **VPM Crime investigation – case management**
  - provide updates of the investigation within the LEAP Case Progress Narrative screen or in Interpose in accordance with **VPM Crime and event reporting and recording**, and
  - comply with the *Victims' Charter Act* and **VPM Victim support**.
- Refer to ReportCyber Investigation Guide and ReportCyber and the CIAU intranet page for further information.

5. Referral to other jurisdictions

5.1 *Interstate referrals - investigations not originating on ReportCyber*

As stated in **VPM Crime attendance – initial action**, where an investigation is transferred to an interstate law enforcement agency (LEA):

- the investigating member must ensure the investigation file is completed and details the reason for the referral
- a supervisor must review the file prior to submission to the work unit manager for approval to release the file to the interstate LEA
- the file must be accompanied by the Referral of Investigation to Interstate Law Enforcement Agency [Form 1418]
- Refer to the interstate LEA contact list on the ICLU intranet site for relevant addresses.

The investigating member must also comply with **VPM Crime investigation – case management**.

5.2 *Interstate referrals via Cybercrime Intelligence Assessment Unit - investigations originating on ReportCyber*

Where a POI has been identified interstate, the investigating member/CIAU must follow the steps in the table below:

Step	Responsibility	Action
1	Investigating member	Ensure an investigation file is completed and details the reason for the referral
2		Submit the investigation file to a supervisor for review prior to submission to the work unit manager for approval to refer the file to the CIAU
3		Email the investigation file to the CIAU via pbea: Crime-CIAU-Mgr and retain all original materials
4		Update LEAP/Interpose
5	CIAU	Create an investigation referral on ReportCyber and request the contact details of the receiving investigation office in the relevant jurisdiction

6		Provide the contact details of the receiving investigation office with the member who was allocated the original report
7	Investigating member	Update LEAP/Interpose with handover details
8		Notify the victim/reporting person

Refer to ReportCyber and the CIAU intranet page for more information.

5.3 *International referrals*

Police members must refer to the Intelligence and Covert Support Command (ICSC), External Agency Liaison - Interpol and Europol intranet page for guidance where it is determined that the matter requires investigation and/or assistance by a jurisdiction outside of Australia.

Related documents

- VPM Crime and event reporting and recording
- VPM Fraud offences
- VPM Crime investigation – case management
- VPM Crime attendance – initial action
- ReportCyber Investigation Guide
- Crime Investigative Guidelines Fraud
- Australia New Zealand Policing Advisory Agency Protocol for Responding to and Managing Cybercrime
- *Victims' Charter Act 2006*

Further advice and information

For further advice and assistance regarding this policy, contact a supervisor or the CIAU, Crime Command via Crime-CIAU-Mgr.

Update history

DATE UPDATED	SUMMARY OF CHANGE	FORCE FILE NUMBER
01/07/2025	This document replaces VPMG Reporting cybercrime. Amendments to update terminology as a consequence of ReportCyber replacing ACORN and CIAU replacing Intelligence Collection and Liaison Unit. Further amendments to clarify existing instructions and for currency.	FF-215481