Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

acma

MEMORANDUM OF UNDERSTANDING CONCERNING THE USE AND OPERATION OF THE REPORTCYBER TRENDS AND REPORTING DASHBOARD MODULE OF THE REPORTCYBER APPLICATION PLATFORM PROVIDED BY THE AUSTRALIAN CYBER SECURITY CENTRE

WITH

THE AUSTRALIAN COMMUNICATIONS AND MEDIA AUTHORITY

ACSC Australian Cyber Security Centre

acma

Table of Contents

Memorandum of Understanding

The Australian Cyber Security Centre (ACSC, part of the Australian Signals Directorate), and the Australian Communications and Media Authority (ACMA) have reached the following understandings.

1. Context

1.1 This Memorandum of Understanding (MOU) is made in the following context:

(i) The Australian Cyber Security Centre is the Australian Government's lead on national cyber security. The ACSC brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age.

(ii) The ReportCyber Application Platform (RCAP) is the back-end platform for ReportCyber, a national online system that enables members of the Australian public to securely report cyber issues and also provide a resource for cyber issue prevention and mitigation. The platform ensures reports submitted through ReportCyber are referred (and potentially re-referred) to the relevant law enforcement jurisdiction(s) for assessment and investigation. The RCAP also provides the Trends and Reporting Dashboard, which provides Participants broader intelligence analysis capability concerning cyber-issue trends. Police jurisdictions access these reports through their own participant interface, which is referred to by police jurisdictions as the RCAP Trends and Reporting Dashboard - *refer Appendix A – ACSC ReportCyber Diagram.*

(iii) The ACMA is a statutory agency established by section 6 of the *Australian Communications and Media Authority Act 2005* (the ACMA Act). The ACMA regulates broadcasting services, radiocommunications, telecommunications, unsolicited communications and certain internet content in Australia. This includes enforcing the C661:2020 Reducing Scam Calls Industry Code to reduce the scale and impact on Australians of scam calls and the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 (the Standard) which requires telecommunications providers to undertake additional identity verification when transferring customers' phone numbers from one telco to another.

(iv) The ACSC has agreed to allow the ACMA access to the RCAP Trends and Reporting Dashboard for the purposes of accessing aggregated ReportCyber data. This data will be used as a source of actionable intelligence by the ACMA.

(v) The ACSC will make the RCAP Trends and Reporting Dashboard module of Report Cyber available to the ACMA based on the understandings contained in this MOU.

2. Definitions

2.1 The Participants have jointly decided upon the following definitions for terms used in this MOU.

ACMA Act means the *Australian Communications and Media Authority Act 2005*.

Confidential Information means information the Participant knows or ought to know is confidential, and includes:

(i) personal information, as that term is defined in the Privacy Act;

(ii) RCAP Information; and

(iii) information the Participants acknowledge in writing to be confidential information for the purpose of this MOU.

Cyber-issue means an issue directed at computing and communications technologies themselves, such as unauthorised access, modification or impairment of electronic communications or data; or issues where the use of the internet or information technology is integral to the event, such as online fraud (eg internet or email scams), online identity theft, cyber bullying, online child exploitation and online intellectual property infringement.

Mobile porting fraud means either the occurrence of a fraudulent mobile number port or an unauthorised SIM swap committed by third-party bad actors.

MOU means this document, including its annexures and schedules (if any).

Participant(s) means the ACMA and ACSC.

Personnel means the Participant's officers, employees, secondees, agents, contractors and subcontractors relevant to this MOU.

Privacy Act means the *Privacy Act 1988* (Cth) as amended from time to time.

ReportCyber means the public-facing national online system that allows the Australian public to securely report cyber issues and also provide advice regarding cyber-issue prevention and mitigation.

RCAP means ReportCyber Application Platform which is the back-end platform for ReportCyber.

RCAP Information means any information which the ACMA has obtained through RCAP.

SIM swap means when a mobile service number is transferred between mobile devices or on the same device i.e., an eSIM swap. A SIM swap does not involve a change in telecommunications provider.

The Standard means the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.

3. Status of MOU

3.1 This MOU is administrative and voluntary in nature. It does not create any legal obligation or legal right (substantive or procedural) that is enforceable by or against either Participant. However, the Participants takes their roles and responsibilities under this document seriously and will endeavour to perform them as if they were legally binding.

3.2 This MOU is intended to work in conjunction with, and not derogate from any other understanding or arrangement that exists between the Participants. To the extent that there are inconsistencies in relation to any matter addressed specifically in this MOU, this MOU will prevail.

3.3 This MOU is not intended to exclude or replace other legal processes on which the Participants may rely to obtain information from another Participant.

4. Objectives of this MOU

4.1 This MOU has been developed to provide a framework to govern the responsibility of the ACMA in relation to its use of RCAP Information.

4.2 The objectives of, and the priority areas of concern for exchange of information under, this MOU are to assist the ACMA in performing its functions and exercising its powers, including but not limited to:

(i) potential serious or systemic non-compliance with the regulatory functions of the ACMA, including the ACMA's enforcement of the Standard which occurs under powers and functions set out in subsection 8(1)(a) of the ACMA Act. This work aligns with the ACSC's cyber security mission as it improves consumer confidence in communications networks and prevents harm arising from unauthorised porting, including where consumer contacts occur online;

(ii) occurrence of actual or suspected mobile number fraud;

(iii) considering the effectiveness of the Standard and identifying any areas of consumer harm that may require consideration of revised or new regulatory safeguards.

5. Guiding principles and use of RCAP

5.1 The ACMA has requested access to the ReportCyber platform to take action in relation to compliance with the Standard, which requires mobile carriage service providers to undertake additional identity verification processes to protect consumers from mobile porting fraud.

5.2 The ACMA may use the RCAP – Trends and Reporting Dashboard as a source of actionable intelligence. Access is provided to the ACMA to provide a more accurate picture in relation to phone scams generally, and specifically in relation to mobile number fraud, including porting and SIM Swap fraud.

5.3 The ACMA recognises the legal and reputational risks that attach to the unauthorised disclosure of information submitted through ReportCyber and will take active steps to minimise the sharing of personally identifiable information, including restricting access to information to Personnel who have a need-to-know in order to achieve the objectives detailed in paragraph 4 of this MOU.

6. Data ownership

6.1 Data submitted through ReportCyber is held by and belongs to the ACSC.

7. Privacy, Security and Confidentiality

7.1 Each Participant is responsible for compliance with its own governing legislation, (including legislation concerning privacy, confidentiality and the sharing of information) and complying with its own internal policies that relates to management of information.

7.2 The ACMA undertakes to maintain current security systems and policies, sufficient to ensure its responsibilities under this MOU are met. In particular, the ACMA will:

(i) ensure appropriate security measures are in place to protect RCAP Information from unauthorised access, use, modification or disclosure;

(ii) only provide access to RCAP to those ACMA Personnel who:

(1) sign an individual Usage Agreement (refer Appendix B) provided by ACSC, the completion of which must be approved by an Executive Level 2 ACMA employee who is responsible for monitoring ACMA staff access to RCAP;

(2) validate ACMA Personnel user accounts to verify that such users have an ongoing need to access the RCAP information and provide ACSC ability to conduct periodic audits to confirm the validation; and

(3) have received training on management and protection of ReportCyber data provided by the ACSC;

(iii) restrict sharing of RCAP Information to ACMA Personnel who have a need to know in order to achieve the objectives in paragraph 4 of this MOU;

(iv) use aggregated or anonymised data where possible;

(v) follow data governance arrangements applicable to the RCAP information as advised by the ACSC from time to time, including those contained in the Usage Agreement;

(vi) have the option to change access control to RCAP for its ACMA Personnel if approved by ACSC;

(vii) share data whether enriched or otherwise with the ACSC where it is permitted to do so under legislation;

(viii) take reasonable steps to ensure that any ACMA Personnel who are authorised to access RCAP do not record, disclose or communicate RCAP Information except in performance of their official duties or as otherwise agreed between the Participants.

7.3 In the event of loss or unauthorised disclosure of Confidential Information, suspected or actual, the Participant in receipt of the Confidential Information shall immediately notify the other Participant. The Participant will immediately undertake such investigations and enquiries into the loss or disclosure as are reasonable in the circumstances and keep the other Participant informed of the progress and outcome of the investigations and enquiries.

8. Disclosure to third parties

8.1 Each Participant acknowledges that every other Participant may be subject to legal processes instituted by third parties which may require the Participant to disclose Confidential Information.

8.2 The exchange of information between the Participants under this MOU remains subject to the applicable law in Australia. To avoid any doubt, this MOU does not authorise the disclosure, use and processing of information for purposes and in a manner other than as allowed under the applicable law. The applicable law in Australia includes the following:

(i) *Freedom of Information Act 1982* (Cth);

(ii) Privacy Act; and

(iii) Part 7A of the ACMA Act.

8.3 If a Participant is permitted or required by law to disclose Confidential Information received from another Participant, the disclosing Participant will:

(i) notify the other Participant as soon as is reasonably practicable, and where possible prior to any disclosure being made, of the disclosure to allow that Participant to take all reasonable steps to maintain the confidentiality or privacy of the information required to be disclosed, including, if necessary and appropriate, making a claim for public interest privilege or requiring a confidentiality undertaking from the person or body to whom the information is required to be disclosed; and

(ii) disclose the Confidential Information only to the extent permitted by or required to comply with the applicable law.

8.4 If a Participant becomes aware that Confidential Information provided by the other Participant is in the public domain, that Participant will inform the other Participant of this as soon as practicable.

8.5 If a Participant, which has received Confidential Information from the other Participant under this MOU, obtains written confirmation from the other Participant that either (a) the information or part of it has been made public, or (b) the other Participant consents to the disclosure of the information or an identified part of it, then the receiving Participant need no longer protect the confidentiality or privacy of that information or the identified part of that information.

8.6 The ACMA will not use RCAP Information to contact individuals in relation to their ReportCyber report unless permission is granted by the ACSC upon written request by the ACMA.

9. Media releases

9.1 Nothing in this paragraph 9 is intended to prevent or restrict the ACMA from making a planned media statement or public announcement regarding a scam or consumer protection issue in general, even if the statement or announcement is based, in whole or in part, on information received through RCAP.

9.2 The ACMA will give the ACSC prior notice of any planned media statements, public announcement or publication that references the ACSC or ReportCyber.

9.3 The ACMA will consult with the ACSC on planned media statements or public announcements which contain information about specific reports made to ReportCyber.

10. Misunderstandings

10.1 Misunderstandings between Participants arising under or relating to this MOU will be resolved at an operational level through negotiations between Participants. If the misunderstanding is unable to be settled at this level, the matter will be escalated without undue delay to an appropriately authorised person with the applicable agency with authority to settle the matter.

11. Costs

11.1 The ACMA will bear its own costs of using RCAP and any activities related to RCAP or conducted under this MOU.

11.2 As the owners of RCAP, the ACSC will take reasonable steps to maintain the system. Nothing in this MOU should be taken as a commitment by the other Participants to fund such maintenance.

12. Commencement, operation, amendment and termination

12.1 Each Participant will carry out activities under this MOU consistent with applicable laws, regulations and policies.

12.2 This MOU will become operative upon signature by the latter of both Participants and remain in effect until it is discontinued in accordance with its terms.

12.3 This MOU may be amended or discontinued at any time by either party, with notice given to the other party.

12.4 The ACSC has, at any time, sole discretion about revoking the ACMA's access to the ReportCyber platform at the individual or agency level.