Australian Payments Plus

Responsible Vulnerability Disclosure Practice

auspayplus.com.au

CONTENTS

1. Introduction and purpose

Australian Payments Plus is committed to maintaining the security and resilience of its systems, products, and services. This Responsible Vulnerability Disclosure Practice provides a clear, safe, and consistent process for security researchers, customers, partners, and the public to report potential security vulnerabilities in our systems.

The objective of this practice is to:

- Encourage responsible, good-faith security research and disclosure
- Reduce the likelihood of vulnerabilities being exploited or disclosed publicly without warning
- Ensure vulnerabilities are assessed, prioritised, and remediated in a timely and coordinated manner

If you believe you have discovered a vulnerability or security issues that impacts the confidentiality, integrity or availability of one of our services or products, we strongly encourage you to submit a report to our security team following the instructions below.

2. Scope

We allow you to conduct vulnerability research and testing only to Australian Payments Plus services and products that are publicly accessible or to which you have lawful access.

For the avoidance of doubt, this practice does not authorise testing of any scheme member, customer, vendor or other third party systems, networks, applications or data. AP+ cannot and does not waive any third-party rights.

Australian Payments Plus Ltd (ABN 19 649 744 203) (AP+), brings together, and is the holding company of Australia's three domestic payment providers, BPAY, eftpos and NPPA. This Responsible Vulnerability Disclosure Practice applies to AP+ in addition to such payment providers and entities as follows:

a) BPAY Group Holding Pty Ltd (ABN 44 626 481 525) - which consists of BPAY Group Pty Ltd (ABN 60 003 311 644) and BPAY Pty Ltd (ABN 69 079 137 518) - manages the BPAY® bill payment service which allows customers to make bill payments through their financial institutions online banking service or via BPAY View and Osko®, a real time payments service that allows users to transfer funds to and from their accounts. Osko leverages the New Payments Platform which is infrastructure provided by NPP Australia Limited. Together, the BPAY entities are referred to as BPAY.
b) ConnectID Pty Ltd (ABN 80 648 970 101) operates a digital identity solution (ConnectID).
c) eftpos Payments Australia Limited (ABN 37 136 180 366) operates the eftpos payment system, which is both a debit card payment system and a prepaid card payment system and Beem which provides a peer-to-peer payments facility/mobile application (eftpos).
d) NPP Australia Limited (ABN 68 601 428 737) operates and manages the real-time account to account payments infrastructure in Australia (NPPA).

Together, AP+, BPAY, ConnectID, eftpos and NPPA are referred to as AP+, we, us, our, throughout this Responsible Vulnerability Disclosure Practice.

3. Out of scope

While we encourage security research on our products and services, the following types of research are strictly prohibited:

- Accessing or attempting to access accounts or information you are not authorised to
- Any attempt to modify or destroy information
- Sending or attempting to send unsolicited or unauthorised email or other type of message
- Conducting social engineering (including phishing) of AP+ employees, contractors, customers or any other related party
- Posting, transmitting, uploading, linking to, sending or storing malware that could impact our services, products or customers
- Exfiltrating, retaining, or disclosing personal, financial, or confidential data beyond what is strictly necessary to confirm the vulnerability
- Clickjacking
- Any physical attempts against AP+ property or data centres
- Weak or insecure SSL ciphers and certificates
- Denial of service (DoS) or stress testing that degrades system availability
- Uncontrolled or high-volume automated scanning that degrades system availability.
- Testing third party websites, applications or services that integrate with our services or products
- Accessing, viewing, copying, extracting, retaining or disclosing any data that is not owned by AP+ (including scheme member, participant, customer or other third-party data).
- Any activity that violates any law

4. Responsibly disclosing a vulnerability

AP+ encourages anyone who identifies a potential security vulnerability to report it promptly.

Reports should be submitted via:

- Email: cybersecurity@auspayplus.com.au
- Subject line: “Responsible Vulnerability Disclosure”

Please include, where possible:

- A clear description of the vulnerability
- Affected product or service, including affected URL(s)
- Date, time and time zone of when the suspected vulnerability was discovered
- Steps to reproduce the vulnerability
- Any relevant screenshots, logs, or proof-of-concept
- Confirmation that you have not retained any data obtained during testing (other than what is strictly necessary to evidence the vulnerability)
- Your contact information

If you feel the email should be encrypted, our PGP key can be found below:

Download PGP key

5. Safe harbour

AP+ considers security research conducted in good faith and in accordance with this practice to be authorised.

AP+ will not:

- request non-disclosure agreements prior to receiving a vulnerability report
- take legal action against security researchers in relation to the discovery and reporting of a potential security vulnerability.

This is provided that all such potential security vulnerabilities are discovered and reported strictly in accordance with this Responsible Vulnerability Disclosure Practice.

Safe harbour will not apply:

- to activities that are intentionally malicious, reckless, or outside the scope of this practice,
- where you access or handle personal information or other data beyond what is strictly necessary to confirm a vulnerability, or where you do not immediately stop and notify AP+ upon encountering data not owned by AP+, or
- where you request, demand, solicit or otherwise initiate negotiations with AP+ for any payment, benefit or other consideration.

6. Disclosure and communication

AP+ requests that vulnerabilities are not publicly disclosed until:

- AP+ has had a reasonable opportunity to investigate and if required remediate the issue, and
- Disclosure timing has been coordinated in good faith with AP+

AP+ will use reasonable endeavours to:

- Acknowledge receipt of vulnerability reports within a reasonable timeframe (i.e., 72 hours)
- Communicate clearly with reporters during assessment and remediation
- Notify reporters when remediation is complete, where contact details are provided

Subject to any regulatory and legal requirements, all reports will be kept confidential, including the details of the potential security vulnerability as well as the identity of all researchers involved in reporting it. Where a report relates to (or may affect) scheme members, customers, vendors or other third parties, AP+ may share relevant details of the report with those parties and/or regulators for investigation, remediation, risk management and legal compliance purposes.

7. Assessment and remediation

AP+ will use reasonable endeavours to ensure all reported vulnerabilities will be:

- Logged and assessed by AP+ Cyber Security
- Prioritised based on risk and potential impact
- Remediated in accordance with AP+ vulnerability management processes

AP+ does not guarantee specific remediation timelines, but remediation will be risk-based and proportionate (as determined by AP+).

8. Privacy

If you have provided your personal information, we may contact you for more information to assist us with investigating your disclosure.

We may also use and disclose your personal information where reasonably necessary to meet our legal and regulatory obligations.

For more information about how we handle your personal information, you can refer to our Australian Payments Plus Privacy Policy.

9. Compensation and recognition

AP+ does **not** operate a bug bounty or offer ongoing monetary rewards for vulnerability disclosure.

We sincerely thank the researchers who have helped keep our customers and communities safe by reporting security vulnerabilities.

AP+ may update this Practice from time to time. Unless AP+ states otherwise, changes take effect when the updated version is published.