Australian Payments Plus

NPP transaction monitoring

Identifying and responding to payments abuse

July 2021

NPP

Terms of use and disclaimer

1. To the fullest extent permitted by law:

    - this document is provided 'AS IS' without warranties of any kind, and NPP Australia Limited (NPPA) neither assumes nor accepts any liability for any errors or omissions contained in this document; and

    - NPPA disclaims all representations and warranties, express or implied, including without limitation, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, as to the specifications set out in this document.

2. You, acknowledge and agree that the information in this document is general only and the suitability and availability of the products or services discussed will vary depending on your financial institution and individual needs. You agree to make and rely solely on your own investigations, and to obtain legal advice, as to the availability, suitability and legal compliance of any implementation of guidance in this document.

3. You must consult your financial institution to ensure that any product or service discussed in this document is supported by that institution prior to taking any steps to implement any guidance in this document.

4. Without limiting the foregoing, this document may provide for the use of technology which may be the subject matter of patents in several countries and/or other intellectual property rights, including copyright, trademark, trade secret and know-how. Any person seeking to implement a solution based on this guidance is solely responsible for determining whether its activities require a licence to such technology. NPPA shall not be liable for any person's infringement of intellectual property rights in connection with the implementation of any guidance in this document.

Third parties wishing to use NPPA registered intellectual property rights including the, Osko, PayTo or PayID trademarks, should visit: www.auspayplus.com.au/brand-portal

NPP Australia reserves the right to modify or amend this document from time to time.

The NPP and customer-provided payment data

Banking applications with integrated NPP payment facilities enable payer customers to send payments in near real time and to enter up to 35 characters of text in the payment reference field and up to 280 characters of narrative with each payment. The data richness of NPP payments is one of the key benefits of the NPP. However, the functionality is also open to misuse by payer customers who may use it to send offensive or abusive messages to payee customers.

Seeing offensive or abusive content in NPP payment messages – even if not intended by the payer customer to be harmful – may cause considerable distress and anxiety to payee customers and to employees of financial institutions. Where a payer customer sends payment messages that include threats to kill or to cause serious harm to the payee customer or another person, they may also commit a criminal offence.

NPP Australia sets standards and rules for financial institutions that participate in NPP. NPP Australia encourages all participating institution to take into account the harm that malicious or careless misuse of NPP payment facilities can cause, and to utilise NPP features and functionality to mitigate this harm. This document describes the NPP features and functionality available.

NPP Transaction monitoring

Offensive and abusive content (payments abuse) may be an indicator of financial abuse. Financial institutions participating in NPP may monitor NPP transactions for a variety of reasons, including to identify indicators of financial abuse and to provide support to vulnerable customers.

The NPP rules therefore permit participating institutions to:

- determine their own standards of what constitutes offensive or abusive content in payment messages; and
- in the case of inbound payments, to use NPP automated alerts (General Investigation Messages) to notify payer institutions of offensive or abusive messages received, whether identified through screening or by the payee customer.

Where a payer institution receives such a General Investigation Message, it is required by the NPP rules to respond to the payee institution within two days and notify the payee institution of any responsive action it proposes to take, such as enforcing its service terms and conditions, cautioning the payer customer or restricting their use of NPP payment messaging capabilities.

Protecting customers from harm

In many cases, it will not be practical or technically feasible for the payer institution to restrict use of NPP messaging capability without restricting the payer's use of mobile or internet payment facilities. Restricting a payer customer's use of payment facilities may end up punishing the payee as much as it punishes the payer, if it means the payer is unable to send the payee critical payments, such as child support payments.

To address this technical challenge, the NPP rules permit payee institutions to withhold – that is, not immediately display - NPP payment data that contain offensive or abusive messages from payee customers. The rules also permit payee institutions to automatically withhold NPP payment messages where the payee customer has made such a request or where it considers withholding messages is necessary to protect its customer. Where messages are withheld, the payee customer must be notified of that fact, the messages must be stored and produced if requested by the payee customer.