# PAYMENT CARD INFORMATION HANDLING PROCEDURE

**Governing Policy**: Payment Card Information Handling Policy

## Purpose

To detail the procedures for payment card information handling.

## Definitions

Unless otherwise defined in this document, all capitalised terms are defined in the glossary.

**CCV** means the **credit card verification** number on each payment card, as follows:

CVC2: 3 digit Card Verification Code (Master card) on signature panel

CVV2: 3 digit Card Verification Value (Visa) on signature panel

CID: Card Identification Number (American Express) above logo on front of card.

**Payment Card** means any credit or debit card accepted by the Australian Institute of Business (AIB).

**Cardholder Data** is Data consisting of the full Primary Account Number (PAN), or data in the form of the full PAN and any of the following: cardholder name, expiration date and/or the CCV number

**PCI DSS** is an acronym for Payment Card Industry Data Security Standard. A Security standard with a set of requirements that must be followed by organisations that handle (accept, transmit, store) payment card data.

**SAQ A** is an acronym for Self-Assessment Questionnaire A (Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced) available at https://www.pcisecuritystandards.org/document_library?category=saqs#results

**VoIP** is an acronym for Voice over Internet Protocol.

**VoIP Facsimile** means transmission of scanned printed material (both text and images) to (or from) a telephone number connected to a device as an email attachment through the Internet.

**Service providers and third-party vendors** means any organisation that processes, transmits or stores cardholder data on behalf of the AIB.

## Procedure

### 1. Acceptable payment methods

1.1. Payment Card payments will only be accepted by AIB via the following payment methods:

(a) Online where cardholder data functions are completely outsourced to validated third parties and audited under SAQ A; and
(b) Telephone payments where cardholder data is entered via payment terminals which are outsourced to validated third parties and audited under SAQ A.

1.2. Companies and individuals must be prevented from providing any cardholder data via an email or VoIP facsimile. If such a request is received:
(a) The email or VoIP fax should be replied to immediately with the credit card number deleted – stating that "AIB does not accept payment card holder information via VoIP fax or email as it is not a secure method of transmitting cardholder data".
(b) The email or fax is to be securely destroyed.

1.3. Cardholder data received via telephone must be processed while the customer is on the line. Writing down a customer's Payment Card information to process at a later time is prohibited. Staff should ensure that conversation is not being recorded while card holder data is collected over the phone.

1.4. AIB does not accept receipt of card holder data on voicemail. In such circumstances:
(a) Staff must immediately delete the message; and
(b) The cardholder should then be contacted and informed that AIB does not process Payment Card information left on voicemail. The customer must also be advised of the acceptable methods of payment under this policy.

## 2. Staff that can handle Payment Card payments

2.1. Only AIB staff that have been appropriately trained and have been approved by the Financial Controller in writing may have access to cardholder data.

2.2. All staff who handle cardholder data will be required to sign an acknowledgement of receipt, understanding and agreement to comply with this policy.

2.3. The Finance Department will maintain a register for the staff who are approved to handle Payment Card payments and will arrange for appropriate training to be conducted at least once a year.

## 3. Storage of cardholder data

3.1 No cardholder data are to be recorded, copied or stored by AIB in hard copy or electronic format under any circumstances.

3.2 Cardholder data is not to be recorded, copied or stored for chargeback purposes.

3.3 Cardholder data is NOT to be recorded, copied, stored, processed or transmitted by AIB on any computers including onto any portable devices, such as USB flash drives, compact disks, personal digital assistants, tablets or phones, in any form. Cardholder information is to be transferred securely and cardholder data is not to be emailed or VoIP faxed either internally or externally.

**Responsibility:**
Financial Controller

| | |
|---|---|
| **Current Status:** | **Version 1** |
| **Approved By:** | Board of Directors |
| **Effective From:** | **3 December 2020** |
| **Date of Approval:** | 3 December 2020 |
| **Previous Versions:** | 26 September 2018 *Payment Card Information Handling Policy V1* |
| **Date of Next Review:** | 3 December 2023 |