



## **Appendix 22: EFTPOS device life cycle standards**

Version 1

Effective date: 2/10/2023

## Document history

**Title:** EFTPOS device life cycle standards

**Version:** 1

**Effective date:** 2/10/2023

**Circulation:** Payments NZ participants, Buddle Findlay, Reserve Bank

The following table summarises amendments to these standards.

Version number and description of amendment	Amendment method and date	Amendment notice date	Effective date of amendment
Version 1: Consolidation of existing device life cycle requirements in the Payments NZ rules and standards.	Board resolution 21 July 23	27 July 23	2 October 23

## Table of contents

<b>Chapter 1: Purpose and overview</b> .....	<b>5</b>
1.1 Payments NZ regulates EFTPOS device life cycle .....	5
1.2 Other Payments NZ rules and standards.....	5
1.3 Copies for non-participants.....	5
<b>Chapter 2: Device registration</b> .....	<b>6</b>
2.1 Purpose of chapter 2.....	6
2.2 Device dates register .....	6
2.3 Device register .....	7
2.4 Registration criteria .....	7
2.5 Application for registration of a model of device.....	8
2.6 Payments NZ response to application.....	8
<b>Chapter 3: Device life cycle dates</b> .....	<b>9</b>
3.1 Purpose of chapter 3.....	9
3.2 No new registrations.....	9
3.3 No new connections.....	10
3.4 Sunset date.....	11
3.5 Sunset date: determination .....	12
<b>Chapter 4: Compromised device</b> .....	<b>13</b>
4.1 Purpose of chapter 4.....	13
4.2 Participant notifies compromise .....	13
4.3 Payments NZ communicates device compromise and instructs .....	14
4.4 Domestic compromise: Payments NZ arranges meeting of affected parties .....	15
4.5 Overseas compromise: Payments NZ arranges meetings CECS MC and board.....	16
4.6 Domestic compromise: affected parties' recommendation to management committee .....	16
4.7 Domestic compromise: acquirer obligations in relation to the affected party meeting .....	17
4.8 Domestic compromise: meetings of CECS and board.....	17
4.9 Management committee recommendation to board .....	18
4.10 Risk management before board decision .....	18
4.11 Board decision .....	19
4.12 No disconnection.....	20
4.13 Disconnection: communication.....	20
4.14 Disconnection: instructions to acquirers .....	21
4.15 Disconnection: method of notification and instruction .....	22
4.16 Acquirer may require early disconnection of a device.....	23
4.17 Payments NZ updates register .....	23
<b>Chapter 5: Device non-compliant</b> .....	<b>24</b>
5.1 Purpose of chapter 5.....	24
5.2 Participant notifies non-compliant model of device.....	24
5.3 Chief executive determines non-compliance .....	24
5.4 Payments NZ arranges meetings of management committee and board.....	25
5.5 CECS management committee makes recommendation to board.....	25
5.6 Board determines action in response to non-compliant model of device .....	26
5.7 Payments NZ communicates decision.....	26
5.8 Disconnection of devices: Payments NZ and acquirer actions .....	27
5.9 Modification of devices.....	27

**Appendix 22A: Compromised device forms .....28**  
**Appendix 22B: Compromised device submission.....40**  
**Appendix 22C: Compromised device disconnection plan.....58**

## Chapter 1: Purpose and overview

### Commentary

#### 1.1 Payments NZ regulates EFTPOS device life cycle

- (1) These standards and the Payments NZ rules regulate the following types of PIN transaction security device (EFTPOS device) to ensure they are secure enough to protect sensitive data on customer cards from unauthorised disclosure or use:
  - (a) PIN entry devices:
  - (b) unattended payment terminals (for example, automated fuel dispensers).
- (2) Only devices of a model registered on the Payments NZ device register may connect to the EFTPOS switching network.
- (3) If Payments NZ removes a model of device from the device register, all devices of the model must disconnect from the EFTPOS switching network.
- (3) These standards specify—
  - (a) in chapter 2—
    - (i) how Payments NZ maintains the device register (and the linked device dates register); and
    - (ii) criteria for registering a model of device on the device register; and
    - (iii) how to apply to Payments NZ to register a model of device; and
  - (b) in chapter 3, how Payments NZ uses 'life cycle dates' to gradually replace older models of device connected to the EFTPOS switching network with newer models of device to keep pace with technological innovation and changes in security threats; and
  - (c) in chapter 4, how Payments NZ removes compromised models of device from the EFTPOS switching network that fail to protect sensitive data on customer cards from unauthorised disclosure or use; and
  - (d) in chapter 5, how Payments NZ deals with deals with models of device that become non-compliant unexpectedly during registration.

#### 1.2 Other Payments NZ rules and standards

- Other Payments NZ rules and standards that regulate terminals and EFTPOS clearing and settlement between participants include the following:
- (a) Part 8A of the rules *CECS: payments instruments*;
  - (b) Part 8B of the rules *CECS: acceptance devices*;
  - (c) Part 8C of the rules *CECS: delivery of payment instructions*;
  - (d) Part 8D of the rules *CECS: EFTPOS authorisation, settlement, and clearing*;
  - (e) appendix 8: *CECS: card standards*;
  - (f) appendix 9: *CECS: EFTPOS procedures*;
  - (g) appendix 10: *CECS: mobile device standards*;
  - (h) appendix 11: *new technology trial standards*;
  - (i) appendix 12: *EFTPOS switching standards*;
  - (j) appendix 13: *terminal standards*.

#### 1.3 Copies for non-participants

- (1) The Payments NZ rules and standards are a multilateral contract between Payments NZ and the participants in its clearing systems.
- (2) A non-participant who seeks access to copies of the rules and standards should contact Payments NZ (who may require the non-participant to sign a standard-form letter that confirms the basis on which the copies will be provided).

## Chapter 2: Device registration

### Standards

---

#### 2.1 Purpose of chapter 2

This chapter specifies how Payments NZ complies with its obligations under rule 8B.14 to—

- (a) maintain and publish a 'device dates register' and a 'device register'; and
  - (b) determine applications for registration of models of device on the 'device register'; and
  - (c) register models of device on the 'device register' that comply with the registration criteria.
- 

#### 2.2 Device dates register

- (1) Payments NZ must maintain a register of device 'life cycle' dates (device dates register) that records—
    - (a) each version of a PIN transaction security standard (security standard), set by a card scheme or the Payments Card Industry (PCI) Security Standards Council (SSC) against which models of device may be registered on the device register (see clause 2.3); and
    - (b) for each version of a security standard recorded, the following life cycle dates determined by the CECS management committee:
      - (i) a 'no new registrations date' determined under clause 3.2 – when Payments NZ stops registering models of device that conform with the version of the security standard;
      - (b) a 'no new connections date' determined under clause 3.3 – when new devices of all registered models that conform with the version of the security standard stop connecting to the EFTPOS switching network for the first time;
      - (c) a 'sunset date' determined under clause 3.4 – when devices of all registered models that conform with the version of the security standard disconnect from the EFTPOS switching network.
  - (2) Payments NZ must publish the device dates register on its public website.
-

**2.3 Device register**

- (1) Payments NZ must maintain a register (device register) that records the models of device that may connect to the EFTPOS switching network.
- (2) For each registered model of device, Payments NZ must record the following details as a minimum:
  - (a) manufacturer:
  - (b) model number:
  - (c) hardware/firmware:
  - (d) version of security standard with which the model conforms:
  - (e) PCI approval number:
  - (f) approval version/class:
  - (g) the following dates determined by the CECS management committee under chapter 3:
    - (i) any no new connections date:
    - (ii) any sunset date.
- (3) If a registered model of device is compromised, Payments NZ must record the following determined by the board under chapter 4:
  - (a) any date from which devices of the model may not connect for the first time to the EFTPOS switching network:
  - (b) any disconnection date.
- (4) If a registered model of device is non-compliant, Payments NZ must record the following determined by the board under chapter 5:
  - (a) any date by which the non-compliant model must be modified to comply with an amendment to the version of the security standard in relation to which it is registered:
  - (b) any disconnection date.
- (5) Payments NZ must publish the device register on its public website.

---

**2.4 Registration criteria**

- On and from 2 April 2013, Payments NZ may only register a model of device on the device register if—
- (a) the applicant gives Payments NZ a letter from the PCI SSC confirming that the model of device conforms with a version of a security standard that is specified on the device dates register; and
  - (b) the date of registration of the model of device is before any 'no new registrations date' determined in accordance with clause 3.2 in relation to the version of the security standard with which the model of device conforms.
-

**2.5 Application for registration of a model of device**

- (1) A person may apply to Payments NZ to register a model of device.
  - (2) On and from 2 April 2013, each application must—
    - (a) be accompanied by a letter from the PCI SSC confirming that the model of device conforms with a version of a security standard that is recorded on the device dates register; and
    - (b) specify the version of the standard with which the model of device conforms.
  - (3) Payments NZ is entitled to rely on the following and is not required to enquire or to independently assess whether or not the model of device complies with the security standard specified in the letter from the PCI SSC provided under subclause (2) —
    - (a) the letter from the PCI SSC provided under subclause (2) confirming that the model of device conforms with a security standard; and
    - (b) information provided by the applicant in respect of the application.
- 

**2.6 Payments NZ response to application**

- (1) As soon as practicable after receipt of an application for registration of a model of device under clause 2.5, Payments NZ must determine whether to approve the application.
  - (2) Payments NZ must approve the application if Payments NZ is satisfied that the application complies with the criteria in clause 2.4.
  - (3) If Payments NZ approves the application, Payments NZ must, as soon as practicable after the decision, record the model of device on the device register.
-



## Chapter 3: Device life cycle dates

### Standards

#### 3.1 Purpose of chapter 3

- (1) This chapter specifies how the CECS management committee exercises its powers under rule 8B.14(1) to determine the following life cycle dates for models of device that conform with an older version of a security standard:
  - (a) no new registrations dates - when Payments NZ stops registering models of device that conform with the version:
  - (b) no new connections dates - when new devices of all registered models that conform with the version stop connecting to the EFTPOS switching network for the first time:
  - (c) sunset dates - when devices of all registered models that conform with the version disconnect from the EFTPOS switching network.
- (2) If the CECS management determines a life cycle date in accordance with rule 8B.14(2), Payments NZ and participants must take the applicable steps specified in this chapter.

#### 3.2 No new registrations

- (1) For each version of a security standard specified on the device dates register, the CECS management committee may, for any reason, determine a date from which Payments NZ will stop registration of models of device that have confirmation from the PCI SSC that the models conform with the version of the standard ('no new registrations date').
- (2) If the CECS management committee determines a no new registrations date under subclause (1), it must, as a minimum, take the following factors into account in determining the date:
  - (a) alignment with life cycles of security standards and standards set by other international bodies, for example, EMVCo:
  - (b) promotion of an interoperable, innovative, safe, open, and efficient CECS:
  - (c) the extent to which unregistered models of the device conforming with the version of the security standard may, if registered, adversely affect the integrity or the reputation of CECS or introduce significant risk into CECS.
- (3) As soon as practicable after the CECS management committee determines a date under subclause (1), Payments NZ must —
  - (a) record the date on the device dates register; and
  - (b) give written notification of the date to CECS participants, switch companies, and device vendors.
- (4) On and from the date determined under subclause (1), Payments NZ must stop registration of models of device that have confirmation from the PCI SSC that the models conform with the version of the security standard to which the determination in subclause (1) relates.

---

**3.3 No new connections**

- (1) For each version of a security standard recorded on the device dates register, the CECS management committee may, for any reason, determine a date on and from which devices of every model of device registered on the device register that conforms with the standard may not connect for the first time to the EFTPOS switching network ('no new connections date').
  - (2) If the CECS management committee determines a no new connections date under subclause (1), it must, as a minimum, take into account the following factors in determining the date:
    - (a) alignment with life cycles of security standards and standards set by other international bodies, for example, EMVCo;
    - (b) promotion of an interoperable, innovative, safe, open, and efficient CECS;
    - (c) the extent to which the models of device may adversely affect the integrity or the reputation of CECS or introduce significant risk into CECS.
  - (3) As soon as practicable after the CECS management committee determines a no new connections date under subclause (1), Payments NZ must,—
    - (a) record the date as follows:
      - (i) for the applicable version of the security standard, on the device dates register;
      - (ii) for the registered models of device that conform with the security standard, on the device register; and
    - (b) give written notification of the date to CECS participants, switch companies, and device vendors.
  - (4) Each acquirer must ensure that, on and from the date determined under subclause (1), its switch does not connect to the EFTPOS switching network for the first time devices of any registered model of device to which the determination relates.
  - (5) Subclauses (1) to (4) do not apply to a new device if—
    - (a) the device replaces a device connected to the EFTPOS switching network before the date determined under subclause (1) that is faulty; or
    - (b) the device is in a new lane in a multi-lane store that uses devices first connected before the date determined under subclause (1); or
    - (c) a merchant operates 2 or more stores and the following apply:
      - (i) all the merchant's stores use devices first connected to the EFTPOS switching network before the date determined under subclause (1);
      - (ii) the device is in a new store opened by the merchant.
-

- 
- 3.4 Sunset date**
- (1) For each version of a security standard specified on the device dates register, the CECS management committee may, for any reason, determine, in accordance with clause 3.5, a sunset date on and from which all devices of every model of device registered on the device register that conforms with the security standard must disconnect from the EFTPOS switching network.
  - (2) If the CECS management committee determines a sunset date under subclause (1), Payments NZ must, as soon as practicable after the determination but no less than 18 months before the sunset date,—
    - (a) record the date as follows:
      - (i) for the applicable version of the security standard, on the device dates register;
      - (ii) for the registered models of device that conform with the security standard, on the device register; and
    - (b) for a sunset date on a date that is 3 years or more following the expiry date of the version of the security standard with which the registered models conform, give written notification of the date to CECS participants and switch companies; and
    - (c) for a sunset date on any other date, give written notification of the date to the following:
      - (i) CECS participants;
      - (ii) switch companies;
      - (iii) each device vendor of every registered model of device that conforms with the version of the security standard to which the sunset date relates.
  - (3) If, for any reason, the CECS management committee determine, in accordance with clause 3.5, that a sunset date determined under subclause (1) (the original sunset date) should be deferred, it may set a later sunset date (the deferred sunset date) instead of the original sunset date.
  - (4) If the CECS management committee determine a deferred sunset date in accordance with subclause (3), Payments NZ must, as soon as practicable after the determination,—
    - (a) record the date as follows:
      - (i) for the applicable version of the security standard, on the device dates register;
      - (ii) for the registered models of device that conform with the security standard, on the device register; and
    - (b) give written notification of the date to CECS participants and switch companies.
  - (5) On the date determined under subclause (1) or subclause (3), as applicable, Payments NZ must remove the models of device from the device register.
  - (6) An acquirer must ensure that, on and from the date determined under subclause (1) or subclause (3), as applicable, its switch disconnects from the EFTPOS switching network all devices of the models of device that conform with the version of the security standard to which the sunset date relates.
-

- 3.5 Sunset date: determination**
- (1) To comply with clause 3.4(1) or, 3.4(3) in the case of a deferred sunset date, the CECS management committee must—
    - (a) take into account the following factors, as a minimum, in determining a sunset date or a deferred sunset date:
      - (i) alignment with life cycles of security standards and standards set by other international bodies, for example, EMVCo;
      - (ii) providing merchants, vendors, device resellers, finance companies, and switches with enough time to disconnect devices and arrange to connect new devices;
      - (iii) promotion of an interoperable, innovative, safe, open, and efficient CECS;
      - (iv) the extent to which the models of device may adversely affect the integrity or the reputation of CECS or introduce significant risk into CECS; and
    - (b) if the sunset date is proposed for a date that is 3 years or more following the expiry date of the version of the security standard with which the registered models of device conform, consult with acquirers and switches; and
    - (c) if the sunset date is proposed for any other date, consult with—
      - (i) acquirers; and
      - (ii) switches; and
      - (iii) each device vendor of every registered model of device that conforms with the version of the security standard to which the sunset date relates; and
    - (d) for a deferred sunset date, consult with acquirers and switches.
  - (2) The CECS management committee must determine the appropriate consultation process to be undertaken with each group identified above (acquirers, switches, and device vendors) depending on—
    - (a) the circumstances of the relevant sunset date and security standard; and
    - (b) the nature of the relationship of each group with Payments NZ; and
    - (c) anything else the CECS management committee believe is relevant to setting the consultation process.
-

## Chapter 4: Compromised device

### Standards

---

#### 4.1 Purpose of chapter 4

This chapter specifies, in accordance with rule 8B.15, the steps in the compromised device process in which Payments NZ determines whether to remove a registered model of device from the device register that has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas.

---

#### 4.2 Participant notifies compromise

### Standards

- (1) A participant must notify Payments NZ if the participant believes that—
  - (a) 1 or more devices of a model registered on the device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas; and
  - (b) the failure is the result of 1 or more attributes of the model of device.
- (2) The participant must give the notification as follows no later than 24 hours after the participant becomes aware of the facts giving rise to the participant's belief:
  - (a) by completing 'compromised device form 1' *Notify Payments NZ of device compromise* at appendix 22A;
  - (b) by sending it to Payments NZ as a pdf document attached to an email message;
  - (c) using the email address for Payments NZ specified on the compromised device contact list.

### Best practice

- (3) If a participant is investigating whether 1 or more attributes of a model of device caused a device compromise, the participant should notify Payments NZ of the investigation (this warns Payments NZ that the participant may notify under subclause (1) and trigger the compromised device process specified in this chapter).
-

## Standards

**4.3 Payments  
NZ  
communicates  
device  
compromise  
and instructs**

- 
- (1) This clause applies to Payments NZ if it—
    - (a) receives a notification from a participant under clause 4.2(1); or
    - (b) decides for any other reason that 1 or more devices of a model registered on the device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas.
  - (2) Payments NZ must, in accordance with subclause (4) notify the following of the notification or the decision referred to in subclause (1) as soon as practicable after receiving the notification or making the decision:
    - (a) CECS participants;
    - (b) the device vendor who applied for registration of the model of device on the device register;
    - (c) every switch company that connects a device of the model of device to the EFTPOS switching network.
  - (3) If the notification given under subclause (2) is in respect of a device that failed to protect sensitive data on a payment instrument in New Zealand, Payments NZ must, in accordance with subclause (4), instruct—
    - (a) every issuer to—
      - (i) identify every payment instrument issued by the issuer that has interacted with the compromised device; and
      - (ii) for every payment instrument identified, determine whether to take any steps in respect of the payment instrument holder to prevent—
        - (A) an adverse effect on the integrity or the reputation of CECS; or
        - (B) the introduction of significant risk into CECS; and
    - (b) the acquirer who acquires transactions from the compromised device, to require the acquirer's switch company to, if requested by an issuer, help the issuer to identify every payment instrument issued by the issuer that has interacted with the device.
  - (4) To comply with subclauses (2) and (3) Payments NZ must—
    - (a) complete 'compromised device form 2' *Payments NZ notifies device compromise and instructs* at appendix 22A; and,
    - (b) send it to the representatives specified on the compromised device contact list for each CECS participant, switch company, and device vendor; and,
    - (c) for each representative, use the email address specified on the compromised device contact list; and
    - (d) send the notice as a pdf document attached to each email message.
  - (5) If an issuer or an acquirer receives an instruction in accordance with subclause (3), the issuer or the acquirer must comply with the instruction as soon as practicable after receipt.
  - (6) Payments NZ may communicate with media, or any other party, in respect of a notification or a decision referred to in subclause (1).
  - (7) If Payments NZ communicates with media in accordance with subclause (6), Payments NZ must notify CECS participants of the communication as soon as practicable after the communication is complete.
-

---

**4.4 Domestic compromise: Payments NZ arranges meeting of affected parties**

- (1) If the notification given under clause 4.3 is in respect of a device that failed to protect sensitive data on a payment instrument in New Zealand, as soon as practicable after Payments NZ has completed giving the notification and the instructions, Payments NZ must, in accordance with subclause (2), ask the following to meet with Payments NZ to complete the device compromise submission in appendix 22B:
    - (a) the device vendor who applied for registration of the model of device on the Payments NZ device register;
    - (b) every switch company that connects a device of the model of device to the EFTPOS switching network;
    - (c) every acquirer who connects a device of the model of device to the EFTPOS switching network;
    - (d) every issuer who has issued a payment instrument that interacted with the compromised device;
    - (e) any qualified person who Payments NZ considers has expertise in the matter.
  - (2) For each affected party specified by subclauses (1)(a) to (d) Payments NZ must—
    - (a) invite the representative(s) for the affected party specified on the compromised device contact list; and
    - (b) use the email address for each specified on the compromised device contact list.
  - (3) If an acquirer receives a request to attend a meeting in accordance with subclause (1), the acquirer must ensure that a representative attends the meeting.
  - (4) If an issuer receives a request to attend a meeting in accordance with subclause (1), the issuer must ensure that a representative attends the meeting.
  - (5) If a switch company receives a request to attend a meeting in accordance with subclause (1), every acquirer using the switch company must require a representative of the switch company to attend the meeting.
  - (6) If Payments NZ arranges a meeting under this clause, Payments NZ must ensure that the meeting commences as soon as practicable after sending all of the requests to attend the meeting but no later than the end of 1 business day after either of the following occur in respect of the model of device—
    - (a) Payments NZ receives notification under clause 4.2(1); or
    - (b) Payments NZ makes a decision under clause 4.3(1)(b).
  - (7) Payments NZ may use the following sample forms in appendix 22A:
    - (a) 'compromised device form 3', *Domestic compromise: notice of meeting of affected parties*;
    - (b) 'compromised device form 4', *Domestic compromise: agenda for meeting of affected parties*.
-

---

**4.5 Overseas compromise: Payments NZ arranges meetings CECS MC and board**

If the notification given under clause 4.3 is in respect of a device that failed to protect sensitive data on a payment instrument overseas, Payments NZ must refer the matter to—

- (a) the CECS management committee to recommend to the board whether to require disconnection of the model of device from the EFTPOS switching network; and
  - (b) as soon as practicable after the CECS management committee makes a recommendation in accordance with paragraph (a), the board to decide at its next scheduled meeting whether to require disconnection of the model of device from the EFTPOS switching network.
- 

**4.6 Domestic compromise: affected parties' recommendation to management committee**

(1) If Payments NZ arranges a meeting of affected parties under clause 4.4, it must require the affected parties to decide whether they have enough information to recommend to the CECS management committee and the board whether to require disconnection of the model of device from the EFTPOS switching network to prevent either or both of the following:

- (a) an adverse effect on the integrity or the reputation of CECS;
- (b) the introduction of significant risk into CECS.

(2) If the affected parties decide that they have enough information to make a recommendation, Payments NZ must—

- (a) ensure that the affected parties complete the device compromise submission specified in appendix 22B no later than 48 hours after any of the following occur in respect to the model of device—
  - (i) Payments NZ receives notification under clause 4.2(1); or
  - (ii) Payments NZ makes a decision under clause 4.3(1)(b); and
- (b) as soon as practicable after receiving the submission, send a copy of the submission to the CECS management committee and to the board.

(3) If the affected parties decide that they do not have enough information to make a recommendation, Payments NZ must—

- (a) ensure that the affected parties complete as much as practicable of the device compromise submission no later than 48 hours after any of the following occur in respect to the model of device—
    - (i) Payments NZ receives notification under clause 4.2(1); or
    - (ii) Payments NZ makes a decision under clause 4.3(1)(b); and
  - (b) as soon as practicable after receiving the incomplete submission, send a copy to the CECS management committee and to the board; and
  - (c) require the affected parties to complete the device compromise submission including the recommendation as soon as practicable; and
  - (d) as soon as practicable after receiving the complete submission, send a copy to the CECS management committee and to the board.
-



**4.7 Domestic compromise: acquirer obligations in relation to the affected party meeting**

- (1) If an acquirer is invited to a meeting of affected parties under clause 4.4, the acquirer must take the following steps in respect of the device compromise submission:
    - (a) use best endeavours to provide the information that Payments NZ requires the acquirer to provide for the device compromise submission as soon as practicable after it requests the information;
    - (b) arrange any reports required by Payments NZ in respect of the device compromised or the merchant operating the device, for example, a forensic report or a police report;
    - (c) provide Payments NZ with details that it requires of the reports;
    - (d) during the period in which the affected parties complete the device compromise submission, determine whether any other device connected to the EFTPOS switching network fails to protect sensitive data on a payment instrument;
    - (e) help Payments NZ to coordinate and lead the meeting of affected parties.
  - (2) If an acquirer's switch company is invited to a meeting of affected parties under clause 4.4, the acquirer must require the switch company to use best endeavours to provide the information that Payments NZ requires the switch company to provide for the device compromise submission as soon as practicable after Payments NZ requests the information.
- 

**4.8 Domestic compromise: meetings of CECS and board**

- As soon as practicable after Payments NZ receives a device compromise submission from the affected parties that contains a recommendation in accordance with clause 4.6, Payments NZ must—
- (a) arrange a meeting of the CECS management committee to recommend to the board whether to require disconnection of the model of device from the EFTPOS switching network; and
  - (b) arrange a meeting of the board to decide whether to require disconnection of the model from the EFTPOS switching network; and
  - (c) ensure that the meeting of the committee occurs before the meeting of the board; and
  - (d) ensure that the meeting of the board occurs—
    - (i) at a time that would reasonably enable the board to decide whether to require disconnection of the model of device; and
    - (ii) no later than 48 hours after Payments NZ receives the submission containing a recommendation.
-

**4.9  
Management  
committee  
recommend  
ation to  
board**

- 
- (1) If a meeting of the CECS management committee is arranged in accordance with clause 4.5 or 4.8 in respect of the failure of 1 or more devices of a model registered on the device register to protect any sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas, the CECS management committee must consider the following:
- (a) for a registered device that failed to protect sensitive data on a payment instrument in New Zealand,—
    - (i) the device compromise submission and any recommendation completed by the affected parties in accordance with clause 4.6; and
    - (ii) any other submission by the affected parties;
  - (b) for a registered device that failed to protect sensitive data on a payment instrument overseas, any submissions from the following:
    - (i) the device vendor who applied for registration of the model of device on Payments NZ's device register;
    - (ii) a switch company who connects devices of the model of device to the EFTPOS switching network;
    - (iii) an acquirer who connects a device of the model of device to the EFTPOS switching network;
    - (iv) an issuer who has issued a payment instrument that interacted with the compromised device;
  - (c) submissions from the following:
    - (i) any other participant;
    - (ii) any other switch company;
    - (iii) any other device vendor;
    - (iv) any other person who the committee considers has a substantial interest in the matter;
  - (d) any response by any other organisation in New Zealand or overseas to the device's failure to protect the sensitive data;
  - (e) the effect on the integrity or the reputation of CECS if—
    - (i) the model of device is disconnected from the EFTPOS switching network; or
    - (ii) the model of device is not disconnected from the EFTPOS switching network.
- (2) The CECS management committee must recommend to the board whether to require disconnection of devices of the relevant model of device from the EFTPOS switching network.
- (3) The CECS management committee may use the sample agenda for the meeting 'compromised device form 5' in appendix 22A.
- 

**Best practice**

**4.10 Risk  
managemen  
t before  
board  
decision**

- 
- (1) This best practice applies to an acquirer if the acquirer believes that a device of a compromised model of device may, if it continues to connect to the EFTPOS switching network in the period before the board decides whether to require disconnection of devices of the compromised model,—
- (a) adversely affect the integrity or the reputation of CECS; or
  - (b) introduce significant risk into CECS.
- (2) The acquirer should, in respect of the acquirer's switch and each merchant with whom the acquirer has a merchant agreement, require the switch and each merchant to—
- (a) stop new connections of devices of the compromised model to the EFTPOS switching network; and
  - (b) disconnect devices of the compromised model from the EFTPOS switching network.
-

## Standards

- 4.11 Board decision**
- (1) At a board meeting arranged under clause 4.5 or 4.8, the board must consider the following:
    - (a) for a device that failed to protect sensitive data on a payment instrument in New Zealand, the device compromise submission and the recommendation completed by affected parties in accordance with clause 4.6;
    - (b) the recommendation of the CECS management committee made in accordance with clause 4.9(2);
    - (c) any response by any other organisation in New Zealand or overseas to the device's failure to protect the sensitive data;
    - (d) submissions from the following:
      - (i) any participant;
      - (ii) any switch company;
      - (iii) any device vendor;
      - (iv) any other person who the board considers has a substantial interest in the matter;
    - (e) the effect on the integrity or the reputation of CECS if—
      - (i) the model of device is disconnected from the EFTPOS switching network; or
      - (ii) the model of device is not disconnected from the EFTPOS switching network.
  - (2) The board must—
    - (a) determine whether to require disconnection of devices of the model from the EFTPOS switching network; and
    - (b) for a device that failed to protect sensitive data on a payment instrument in New Zealand, make the determination no later than 48 hours after Payments NZ received a submission containing a recommendation.
  - (3) If the board decides to require disconnection of devices of the model from the EFTPOS switching network,—
    - (a) the board must determine the following, having regard to advice from any person who the board considers has a substantial interest in the matter,:
      - (i) a date from which devices of the model may not connect for the first time to the EFTPOS switching network;
      - (ii) a date from which devices of the model must disconnect from the EFTPOS switching network; and
    - (b) Payments NZ must, as soon as practicable after the board makes a decision, take the steps specified in clauses 4.12 to 4.17.
  - (4) To avoid doubt the board must apply the determination under subclause (3)(a)(i) to all new devices of the model including without limit a device if—
    - (a) the device replaces a device connected before the date determined under subclause (3)(a)(i) that is faulty; or
    - (b) the device is in a new lane in a multi-lane store that uses devices first connected to the EFTPOS switching network before the date determined under subclause (3)(a)(i); or
    - (c) a merchant operates 2 or more stores and the following apply:
      - (i) all the merchant's stores use devices first connected to the EFTPOS switching network before the date determined under subclause (3)(a)(i);
      - (ii) the device is in a new store opened by the merchant .
  - (5) To avoid doubt the board may, for any reason, determine under subclause (3)(a)(ii) that devices of the model—
    - (a) must be disconnected immediately; and
    - (b) may be disconnected whether or not the PCI SSC has removed the model from the PCI SSC's list of approved devices.
  - (6) The board may use the sample agenda for the meeting 'compromised device form 6 in appendix 22A.

**4.12 No disconnection**

- (1) If the board decides under clause 4.11 not to require disconnection of devices of a model from the EFTPOS switching network, Payments NZ must, in accordance with subclause (2), notify the following of the board's decision:
    - (a) each CECS participant:
    - (b) the device vendor who applied for registration of the model on the Payments NZ device register:
    - (c) every switch company who connects a device of the model to the EFTPOS switching network.
  - (2) To comply with subclause (1) Payments NZ must—
    - (a) complete 'compromised device form 7' *Payments NZ notice: device not disconnected* at appendix 22A; and
    - (b) send it to each person specified in subclause (1) using the applicable representatives and email addresses specified on the compromised device contact list; and
    - (c) attach the notice as a pdf document to each email message.
- 

**4.13 Disconnection: communication**

- If the board decides under clause 4.11 to require disconnection of devices of a model from the EFTPOS switching network, Payments NZ—
- (a) must, in accordance with clause 4.15, notify the following of the board's decision, the date from which devices of the model may not connect for the first time to the EFTPOS switching network and the disconnection date:
    - (i) CECS participants:
    - (ii) the device vendor who applied for registration of the model of device on the Payments NZ device register:
    - (iii) every switch company who connects a device of the model to the EFTPOS switching network; and
  - (b) may communicate with media, or any other party, in respect of the board's decision; and
  - (c) must give communication guidelines to the following in respect of the board's decision:
    - (i) to every acquirer for communicating with media or with merchants with whom the acquirer has a merchant agreement:
    - (ii) to every issuer for communicating with media or with customers to whom the issuer has issued a payment instrument.
-

**4.14****Disconnection:  
instructions to  
acquirers**

- 
- (1) If the board decides under clause 4.11 to require disconnection of devices of a model from the EFTPOS switching network, Payments NZ must, in accordance with clause 4.15, give the instructions in subclauses (2) to (4) to every acquirer.
  - (2) Payments NZ must instruct each acquirer to require the acquirer's switch company to—
    - (a) notify the acquirer of the name of every merchant who has a merchant agreement with the acquirer and who operates a device of the compromised model of device; and
    - (b) manage and monitor the process for disconnection of devices of the compromised model from the EFTPOS switching network and replacement with devices of a different model; and
    - (c) manage communications with the device vendor of the compromised model of device in respect of the disconnection and replacement process; and
    - (d) during the disconnection and replacement process, notify Payments NZ when required by Payments NZ of the number of devices disconnected and replaced; and
    - (e) from the date determined by the board, prevent every device of the model of device from connecting for the first time to the EFTPOS switching network including, without limit, a new device if—
      - (i) the device replaces a device connected before the date determined by the board that is faulty; or
      - (ii) the device is in a new lane in a multi-lane store that uses devices first connected to the EFTPOS switching network before the date determined by the board; or
      - (iii) a merchant operates 2 or more stores and the following apply:
        - (A) all the merchant's stores use devices first connected to the EFTPOS switching network before the date determined by the board;
        - (B) the device is in a new store opened by the merchant; and
    - (f) no later than the disconnection date determined by the board, disconnect devices of the compromised model of device from the EFTPOS switching network.
  - (3) Payments NZ must instruct each acquirer to notify every merchant identified in accordance with subclause (2)(a)—
    - (a) of the board's decision to disconnect the compromised model of device from the EFTPOS switching network; and
    - (b) that the merchant will require a replacement device of a different model of device no later than the disconnection date.
- 

*(clause 4.14 continued on next page)*

---

**4.14**  
**Disconnection:**  
**instructions to**  
**acquirers**  
(continued)

- (4) Payments NZ must instruct each acquirer to require its switch company to require the vendor of the compromised model of device to—
- (a) determine the number of devices of the compromised model of device to be disconnected from the EFTPOS switching network and replaced with a different model of device; and
  - (b) confirm whether or not the vendor can replace every device of the compromised model with a different model of device no later than the disconnection date; and
  - (c) determine any functional differences between the compromised model of device and the replacement model of device and ensure that the replacement model provides at least equal functionality to the compromised model; and
  - (d) if the replacement model of device is not registered on the Payments NZ device register, apply to Payments NZ to register the replacement model of device in accordance with clause 2.5; and
  - (e) if the replacement model of device requires approval from any other entity before devices of the model are connected to the EFTPOS switching network, arrange to get the approval from the entity; and
  - (f) arrange a process for disconnection of devices of the compromised model and replacement with devices of the replacement model; and
  - (g) communicate with device resellers in respect of the process at paragraph (f); and
  - (h) send devices of the replacement model to device resellers and the merchants identified in accordance with subclause (2)(a); and
  - (i) require device resellers to replace devices of the compromised model with devices of the replacement model.
- (5) Each acquirer must comply with every instruction given under this clause.
- 

**4.15**  
**Disconnection:**  
**method of**  
**notification and**  
**instruction**

- (1) If the board decides under clause 4.11 to require disconnection of devices of a model from the EFTPOS switching network, Payments NZ must take the steps in subclause (2) to comply with its obligations to—
- (a) notify the decision under clause 4.13(a); and
  - (b) instruct acquirers under clause 4.14.
- (2) Payments NZ must—
- (a) complete 'compromised device form 8' *Payments NZ notice and instructions: device disconnected* at appendix 22A; and
  - (b) send it to the representatives specified on the *compromised device contact list* of CECS participants, switch companies, and device vendors; and
  - (c) for each representative, use the email address specified on the *compromised device contact list*; and
  - (d) send the notice as a pdf document attached to each email message.
-

**4.16 Acquirer may require early disconnection of a device**

- (1) This clause applies to an acquirer if—
    - (a) the acquirer receives a notification from a switch company under clause 4.14(2)(a) of the name of a merchant with whom the acquirer has a merchant agreement and who operates a device of the compromised model of device; but
    - (b) the acquirer believes that the device may, if it continues to connect to the EFTPOS switching network until the disconnection date,—
      - (i) adversely affect the integrity or the reputation of CECS; or
      - (ii) introduce significant risk into CECS.
  - (2) The acquirer must—
    - (a) notify the following of the name of the merchant:
      - (i) Payments NZ;
      - (ii) the acquirer's switch company;
      - (iii) the device vendor; and
    - (b) require the acquirer's switch company to, as soon as practicable after sending the notification, disconnect the compromised model of device from the EFTPOS switching network.
- 

**4.17 Payments NZ updates register**

- (1) If the board decides to require disconnection of devices of a model from the EFTPOS switching network, Payments NZ must record the following on the device register determined by the board in accordance with clause 4.11(3):
    - (a) the date from which devices of the model of device may not connect for the first time to the EFTPOS switching network;
    - (b) the date from which devices of the model must disconnect from the EFTPOS switching network.
  - (2) On the disconnection date, Payments NZ must remove the model of device from the device register.
-

## Chapter 5: Device non-compliant

### Standards

<b>5.1 Purpose of chapter 5</b>	<p>This chapter specifies, in accordance with rule 8B.16, the steps in the 'non-compliant model of device process' in which Payments NZ determines whether to remove a registered model of device from the device register because—</p> <ul style="list-style-type: none"> <li>(a) the PCI SSC amends, or proposes to amend, the version of the security standard in relation to which it is registered on and from a specified date (that is before the sunset date determined under clauses 3.4 and 3.5 for all models of device registered in relation to the version of the security standard); and</li> <li>(b) on the specified date, the registered model will no longer conform with the version of the security standard (and, accordingly, no longer meet all the registration criteria specified in clause 2.4).</li> </ul>
<b>5.2 Participant notifies non-compliant model of device</b>	<ul style="list-style-type: none"> <li>(1) For a non-compliant model of device to which this chapter applies, a participant must notify Payments NZ as follows if the participant believes— <ul style="list-style-type: none"> <li>(a) before the amendment date of the version of the security standard, that the model of device is unlikely to comply with the proposed amendment; or</li> <li>(b) on or after the amendment date, that the model of device does not comply with the amended security standard.</li> </ul> </li> <li>(2) The participant must give the notification as follows: <ul style="list-style-type: none"> <li>(a) by email;</li> <li>(b) to the chief executive and the manager, clearing systems;</li> <li>(c) no later than 24 hours after becoming aware of the facts giving rise to the participant's belief.</li> </ul> </li> </ul>
<b>5.3 Chief executive determines non-compliance</b>	<p>The Payments NZ chief executive may decide for any reason that a registered model of device is non-compliant.</p>



- 
- 5.4 Payments NZ arranges meetings of management committee and board**
- (1) Payments NZ must take the steps specified by this clause if—
    - (a) it receives a notification from a participant under clause 5.2; or
    - (b) the chief executive decides under clause 5.3 that a registered model of device is non-compliant.
  - (2) Payments NZ must take the steps as soon as practicable after—
    - (a) it receives the notification; or
    - (b) the chief executive makes the decision.
  - (3) Payments NZ must arrange a meeting of—
    - (a) the CECS management committee to recommend to the board, in accordance with clause 5.5, the most appropriate action in respect of the non-compliant model of device; and
    - (b) the board to determine, in accordance with clause 5.6, the most appropriate action in respect of the non-compliant model of device.
  - (4) Payments NZ must ensure that—
    - (a) the meeting of the CECS management committee occurs—
      - (i) before the meeting of the board; but
      - (ii) as soon as practicable after Payments NZ receives the notification or the chief executive makes the decision (whichever is the earlier); and
    - (b) the meeting of the board occurs as soon as practicable after the CECS management committee has agreed its recommendation to the board.
- 

- 5.5 CECS management committee makes recommendation to board**
- (1) At a CECS management committee arranged under clause 5.4, the committee must recommend to the board the most appropriate action in respect of the non-compliant model of device to prevent—
    - (a) an adverse effect on the integrity or the reputation of CECS; or
    - (b) the introduction of significant risk into CECS.
  - (2) In making a recommendation under subclause (1), the committee may consider the following:
    - (a) the number of devices of the non-compliant model connected to the EFTPOS switching network;
    - (b) whether to recommend the following:
      - (i) modification of devices of the non-compliant model to comply with the amendment to the version of the security standard in relation to which the model is registered;
      - (ii) re-registration of the non-compliant model on the device register (and, if applicable, any re-registration date);
      - (iii) removal of the non-compliant model from the device register and disconnection of every device of the non-compliant model from the EFTPOS switching network (and, if applicable, any disconnection date);
    - (c) submissions from the following:
      - (i) any CECS participant;
      - (ii) the device vendor who applied for registration of the non-compliant model on the device register;
      - (iii) any switch company who connects a device of the non-compliant model to the EFTPOS switching network.
-

---

**5.6 Board determines action in response to non-compliant model of device**

- (1) At a board meeting arranged under clause 5.4, the board must determine the most appropriate action in respect of the non-compliant model of device to prevent—
    - (a) an adverse effect on the integrity or the reputation of CECS; or
    - (b) the introduction of significant risk into CECS.
  - (2) In making a decision under subclause (1), the board—
    - (a) must consider the recommendation of the CECS management committee made in accordance with clause 5.5; and
    - (b) may consider submissions from the following:
      - (i) any CECS participant;
      - (ii) the device vendor who applied for registration of the non-compliant model on the device register;
      - (iii) any switch company who connects a device of the non-compliant model to the EFTPOS switching network.
  - (3) The board may, for any reason, decide to require—
    - (a) removal of the non-compliant model from the device register; and
    - (b) disconnection of all devices of the non-compliant model from the EFTPOS switching network.
  - (4) To avoid doubt the board may, for any reason, determine under subclause (3) that devices of the model—
    - (a) must be disconnected immediately; and
    - (b) may be disconnected whether or not the PCI SSC has removed the model from the PCI SSC's list of approved devices.
  - (5) If the board decides to require disconnection of devices of the non-compliant model from the EFTPOS switching network under subclause (3), the board must determine a date on and from which all devices of the non-compliant model of device must disconnect from the EFTPOS switching network.
- 

**5.7 Payments NZ communicates decision**

- As soon as practicable after the board makes a decision under clause 5.6, Payments NZ must notify the following of the board's decision by email:
- (a) the CECS management committee (representatives for each participant and infrastructure member);
  - (b) CECS participants (nominated office holders of each participant organisation represented on the CECS management committee);
  - (c) the device vendor who applied for registration of the non-compliant model of device on the device register (using the primary contact person for the device vendor specified on the device registration application form);
  - (d) every switch company who connects a device of the non-compliant model of device to the EFTPOS switching network (if the switch company is an infrastructure member, to the infrastructure member of the CECS management committee).
-

**5.8  
Disconnection  
of devices:  
Payments NZ  
and acquirer  
actions**

- 
- (1) If the board decides to require disconnection of all devices of a non-compliant model of device from the EFTPOS switching network under clause 5.6,—
    - (a) the following apply to Payments NZ and to acquirers as if the board had decided to disconnect all devices of a compromised model of device from the EFTPOS switching network under clause 4.11:
      - (i) to Payments NZ, clauses 4.13, 4.14(1) to (4), and 4.15;
      - (ii) to acquirers, clauses 4.14(5) and 4.16; and
    - (b) Payments NZ must as soon as practicable after the decision,—
      - (i) record the disconnection date on the device register; and
      - (ii) give public notice on the Payments NZ website of the disconnection date.
  - (2) On the disconnection date determined under clause 5.6, Payments NZ must remove the non-compliant model of device from the device register.
  - (3) Each acquirer must ensure that, on and from the disconnection date, its switch disconnects from the EFTPOS switching network all devices of the non-compliant model of device.
- 

**5.9  
Modification of  
devices**

- (1) If the board decides to require modification of any non-compliant model of device under clause 5.6 from a specified date, as soon as practicable after the decision, Payments NZ must amend and update the device register to record the specified date.
  - (2) Subclause (3) applies to Payments NZ if the board decides to require both of the following under clause 5.6 in relation to the same version of a security standard amended (or proposed to be amended) before the sunset date determined under clause 3.4—
    - (a) disconnection of any non-compliant model of device registered in relation to the security standard; and
    - (b) modification of any non-compliant model of device registered in relation to the security standard to comply with the amended security standard.
  - (3) As soon as practicable after the decision, Payments NZ must amend and update the device register to clearly—
    - (a) communicate the board's decision to require both disconnection and modification of non-compliant models of device registered in relation to the same security standard; and
    - (b) identify every model that—
      - (i) must disconnect; and
      - (ii) must be modified.
-

## Appendix 22A: Compromised device forms

### Commentary

---

**Purpose** This appendix specifies the forms participants and Payments NZ use during the compromised device process specified in chapter 4 of the EFTPOS device life cycle standards when a device fails to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas.

---

**Contents** This appendix contains the following forms:

Form number	Title
1	Notify Payments NZ of device compromise
2	Payments NZ notifies device compromise and instructs
3	Domestic compromise: notice of meeting of experts
4	Domestic compromise: agenda for meeting of experts
5	Domestic compromise: agenda for a meeting of the CECS management committee
6	Domestic compromise: agenda for a meeting of the board
7	Payments NZ notice: device not disconnected
8	Payments NZ notice and instructions: device disconnected

---

Standards

Compromised device form 1  
 Notify Payments NZ of device compromise

Confidential – High Priority

To: Payments NZ Limited, mailto: [SteveW@paymentsnz.co.nz](mailto:SteveW@paymentsnz.co.nz),

From:

Date of notice:

We notify you that we believe that 1 or more devices of the following model registered on the Payments NZ Ltd device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas:

Manufacturer:

Model:

PCI version no.:

Product type:

Is the device compromised in New Zealand or overseas?

Date we became aware of the compromise:

Details of the compromise:

Contact information:

Name:

Title:

Phone:

Email:

## Compromised device form 2 Payments NZ notifies device compromise and instructs

Confidential – High Priority

**From:** Payments NZ Limited, 04 890 6754, [SteveW@paymentsnz.co.nz](mailto:SteveW@paymentsnz.co.nz),

**To:** [representatives on the compromised device contact list]

**Date of notice:** \_\_\_\_\_

We notify you under clause 4.3 of the EFTPOS device life cycle standards that [Payments NZ has received notification/ or Payments NZ has decided] that 1 or more devices of the following model registered on the device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas:

**Manufacturer:**

**Model:**

**PCI version no.:**

**Product type:**

**The device compromised is located in New Zealand / overseas)**

**Date of notification received or date of Payments NZ's decision**

**Details of the compromise:**

**If the compromised device is in New Zealand:**

**Instructions to issuers: You must do the following:**

- Identify every card and every payment application on a mobile device that you have issued that has interacted with the compromised device.
- In respect of each card and each payment application on a mobile device that has interacted with the compromised device, determine whether to take any steps to prevent—
  - an adverse effect on the integrity or the reputation of CECS; or
  - the introduction of significant risk into CECS(e.g. notifying a cardholder of the interaction with the device or cancelling the card).

**Instruction to an acquirer who acquires transactions from the compromised device: You must:**

- Require your switch to help issuers who ask the switch to identify cards or payment applications on mobile devices that the issuers have issued and that have interacted with the compromised device.

Compromised device form 3  
Domestic compromise: notice of meeting of affected parties

Confidential – High Priority

From: Payments NZ Limited, 04 890 6754, [SteveW@paymentsnz.co.nz](mailto:SteveW@paymentsnz.co.nz),

To: [representatives of affected parties on the compromised device contact list]

Date of notice: \_\_\_\_\_

**Subject:** Meeting to recommend whether to disconnect a compromised model of device

We refer to the attached notification [attach compromise device form 2] about the failure of a device to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand.

In accordance with clause 4.4 of the EFTPOS device life cycle standards, we request you to attend a meeting at [time] on [date] at [place] to determine whether to disconnect the model of device from the EFTPOS switching network.

I also attach:

- an agenda for the meeting; and
- a template we will use at the meeting to—
  - review the causes and consequences of the device’s failure to protect sensitive data on a payment instrument; and
  - recommend whether or not to disconnect the model of device from the switching network.

## Compromised device form 4 Domestic compromise: agenda for meeting of affected parties

Confidential – High Priority

**Date:** \_\_\_\_\_

**Time:** \_\_\_\_\_

**Venues:** Payments NZ Limited, Level 6, Simpl House, 40 Mercer Street, Wellington  
Payments NZ Limited, Level 17, AIG Building, 41 Shortland Street, Auckland

### **Conference call numbers:**

New Zealand (toll free): 0508 55 22 11

Australia (toll free): 1800 150 421

Metered Access: +64 977 2493

Guest Pass code: 724820811156

### **Agenda:**

#### **1. Notice of meeting – for noting**

Payments NZ's chief executive notes that Payments NZ gave notice of the meeting of affected parties in accordance with clause 4.4 of the EFTPOS device life cycle standards.

#### **2. Summary – for noting**

Payments NZ's chief executive notes—

- a device of a model of device registered on the device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand; and
- the details of the device and the failure; and
- that the affected parties must complete the submission attached to the agenda and include a recommendation to Payments NZ's CECS management committee and board as to whether to disconnect the model of device from the EFTPOS switching network.

#### **3. Compromised device submission – for decision**

The affected parties must decide in accordance with clause 4.6 of the EFTPOS device life cycle standards whether the affected parties have enough information to recommend to the CECS management committee whether to require disconnection of the model of device from the EFTPOS switching network to prevent either or both of the following:

- an adverse effect on the integrity or the reputation of the consumer electronic clearing system;
- the introduction of significant risk into the consumer electronic clearing system.

---

Company secretary

Attached:

Compromised device submission template



## Compromised device form 5 Agenda for a meeting of the CECS management committee

Confidential – High Priority

**Date:** \_\_\_\_\_

**Time:** \_\_\_\_\_

**Venues:** Payments NZ Limited, Level 6, Simpl House, 40 Mercer Street, Wellington  
Payments NZ Limited, Level 17, AIG Building, 41 Shortland Street, Auckland

**Conference call numbers:**

New Zealand (toll free): 0508 55 22 11

Australia (toll free): 1800 150 421

Metered Access: +64 977 2493

Guest Pass code: 724820811156

**Agenda:**

**1. Notice – for noting**

The Chair confirms that a quorum is present (under clause 27.7(c) of Payment NZ Limited's constitution). The Chair declares that notice of the CECS management committee meeting has been given in accordance with Payments NZ's rules.

**2. Summary – for noting**

The Chair or the chief executive report that—

- a device of a model of device registered on the device register has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use [in New Zealand/overseas]; and
- the details of the device and the failure; and
- the committee must recommend to the board whether to require disconnection of devices of the relevant model of device from the EFTPOS switching network.

**3. Submissions and effect of disconnection – for noting**

The committee must note—

- for a registered device that failed to protect sensitive data on a payment instrument in New Zealand,—
  - the device compromise submission and any recommendation completed by the affected parties in accordance with clause 4.6 of the EFTPOS device life cycle standards; and
  - any other submission by the affected parties; and
- for a registered device that failed to protect sensitive data on a payment instrument overseas, any submissions from the following:
  - the device vendor who applied for registration of the model of device on the Payments NZ device register;
  - a switch company who connects devices of the model of device to the EFTPOS switching network;
  - an acquirer who connects devices of the model of device to the EFTPOS switching network;
  - an issuer who has issued a payment instrument that interacted with the compromised device; and
- submissions from the following:

- any other participant:
- any other switch company:
- any other device vendor:
- any other person who the committee considers has a substantial interest in the matter; and
- any response by any other organisation in New Zealand or overseas to the failure of the device to prevent unauthorised disclosure or use of sensitive data on a payment instrument; and
- the effect on the integrity or the reputation of the consumer electronic clearing system if—
  - the model of device is disconnected from the EFTPOS switching network; or
  - the model of device is not disconnected from the EFTPOS switching network.

#### **4. Recommendation - for decision**

The management committee must recommend to the board whether to require disconnection of devices of the relevant model of device from the EFTPOS switching network.

---

Company secretary

Attached:

Compromised device submission

## Compromised device form 6 Agenda for a meeting of the board

Confidential – High Priority

**Date:** \_\_\_\_\_

**Time:** \_\_\_\_\_

**Venues:** Payments NZ Limited, Level 6, Simpl House, 40 Mercer Street, Wellington  
Payments NZ Limited, Level 17, AIG Building, 41 Shortland Street, Auckland

**Conference call numbers:**

New Zealand (toll free): 0508 55 22 11

Australia (toll free): 1800 150 421

Metered Access: +64 977 2493

Guest Pass code: 724820811156

**Agenda:**

**1. Notice – for noting**

The Chair confirms that all directors have been notified of the meeting in accordance with the Payments NZ rules. The Chair confirms that a quorum is present (under clause 22.4 of Payments NZ Limited’s constitution i.e. at least three quarters of directors entitled to vote at the meeting are present in person or by alternate director).

The Chair declares under clause 22.2(c) of the constitution that—

- the meeting is necessary as a matter of urgency; and
- the Chair waives the requirement that each director is to be given not less than 10 business days’ notice of the meeting; and
- at least 3 hours’ notice of the meeting has been given.

The Chair notes the names of representatives from other people attending as observers.

**2. Summary – for noting**

The Chair and/or the chief executive report that—

- a device of a model of device registered on the EFTPOS switching network has failed to protect sensitive data on a payment instrument from unauthorised disclosure or use [in New Zealand/overseas]; and
- the details of the device and the failure; and
- the board must decide whether to require disconnection of devices of the relevant model of device from the EFTPOS switching network.

### **3. Submissions and effect of disconnection – for noting**

The board notes—

- for a registered device that failed to protect sensitive data on a payment instrument in New Zealand, the device compromise submission completed in accordance with clause 4.6 of the EFTPOS device life cycle standards; and
- a recommendation from the CECS management committee; and
- submissions from the following:
  - any participant;
  - any switch company;
  - any device vendor;
  - any other person who the board considers has a substantial interest in the matter; and
- any response by any other organisation in New Zealand or overseas to the failure to of the device to prevent unauthorised disclosure or use of sensitive data on a payment instrument; and
- the effect on the integrity or the reputation of the consumer electronic clearing system if—
  - the model of device is disconnected from the EFTPOS switching network; or
  - the model of device is not disconnected from the EFTPOS switching network.

### **4. Board decision**

The board determines whether or not to require disconnection of devices of the model from the EFTPOS switching network.

If the board decides to require disconnection of devices of the model from the EFTPOS switching network, the board determines the following having regard to advice from any person who the board considers has a substantial interest in the matter:

- a date from which devices of the model of device may not connect for the first time to the EFTPOS switching network;
- a date from which devices of the model must disconnect.

---

Company secretary

Attachments:

Compromised device submission

Compromised device form 7  
Payments NZ notice: device not disconnected

Confidential – High Priority

**From:** Payments NZ Limited, 04 890 6754, [SteveW@paymentsnz.co.nz](mailto:SteveW@paymentsnz.co.nz),

**To:** [representatives on the compromised device contact list]

**Date of notice:** \_\_\_\_\_

We refer to the attached notification [attach compromise device form 2] about the failure of the device specified in the notice to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand [or overseas].

In accordance with clause 4.12 of the EFTPOS device life cycle standards, Payments NZ notifies you that the board has decided not to require disconnection of devices of the model from the EFTPOS switching network.

If you have any questions about this notice, please contact Payments NZ Limited on (04) 890 6750.

## Compromised device form 8 Payments NZ notice and instructions: device disconnected

Confidential – High Priority

**From:** Payments NZ Limited, 04 890 6754, [SteveW@paymentsnz.co.nz](mailto:SteveW@paymentsnz.co.nz),

**To:** [representatives on the compromised device contact list]

**Date of notice:** \_\_\_\_\_

We refer to the attached notification [attach compromise device form 2] about the failure of the device specified in the notice to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand [or overseas].

In accordance with clause 4.13 of the EFTPOS device life cycle standards, Payments NZ notifies you that the board has decided—

- to require disconnection of devices of the model from the EFTPOS switching network no later than [insert time and date of disconnection]; and
- that no devices of the model of device may connect for the first time to the EFTPOS switching network on and from [insert no new connections date]

In accordance with clause 4.14 of the EFTPOS device life cycle standards, Payments NZ instructs every acquirer to take the following steps:

**You must require your switch to:**

- Tell you the name of every merchant with whom you have a merchant agreement and who operates a device of the compromised model of device.
- Manage and monitor the process for disconnection of devices of the compromised model from the EFTPOS switching network and replacement with devices of a different model.
- Manage communications with the vendor of the compromised model of device in respect of the disconnection and replacement process.
- During the disconnection and replacement process, notify Payments NZ when required by Payments NZ of the number of devices disconnected and replaced.
- From the no new connections date, prevent every device of the compromised model from connecting for the first time to the EFTPOS switching network including a device if—
  - the device replaces a device connected before the no new connections date that is faulty; or
  - the device is in a new lane in a multi-lane store that uses devices first connected to the EFTPOS switching network before the no new connections date; or
  - a merchant operates 2 or more stores and the following apply—
    - all the merchant’s stores use devices first connected to the EFTPOS switching network before the date determined by the board; and

- the device is in a new store opened by the merchant.
- Disconnect devices of the compromised model of device from the EFTPOS switching network no later than the disconnection date.

**You must tell every merchant with whom you have a merchant agreement and who operates a device of the compromised model:**

- Of the board's decision to disconnect the compromised model of device from the EFTPOS switching network.
- That the merchant will require a replacement device of a different model of device no later than the disconnection date.

**You must require your switch to require the vendor of the compromised model of device to:**

- Determine the number of devices of the compromised model of device to be disconnected from the EFTPOS switching network and replaced with a different model of device.
- Confirm whether or not the vendor can replace every device of the compromised model with a different model of device no later than the disconnection date.
- Determine any functional differences between the compromised model of device and the replacement model of device and ensure that the replacement model provides at least equal functionality to the compromised model.
- If the replacement model of device is not registered on the Payments NZ device register, apply to Payments NZ to register the replacement model of device.
- If the replacement model of device requires approval from any other entity before devices of the model are connected to the EFTPOS switching network, arrange to get the approval from the entity.
- Arrange a process for disconnection of devices of the compromised model and replacement with devices of the replacement model.
- Communicate with device resellers in respect of the swap out process.
- Send devices of the replacement model to device resellers and the merchants.
- Require device resellers to replace devices of the compromised model with devices of the replacement model.

If you have any questions about this notice, please contact Payments NZ Limited on (04) 890 6750.

## Appendix 22B: Compromised device submission

**Purpose:** The EFTPOS device life cycle standards, clause 4.6 *Domestic compromise: affected parties' recommendation to management committee* provides:

- (1) If Payments NZ arranges a meeting of affected parties under clause 4.4, it must require the affected parties to decide whether they have enough information to recommend to the CECS management committee and the board whether to require disconnection of the model of device from the EFTPOS switching network to prevent either or both of the following:
  - (a) an adverse effect on the integrity or the reputation of CECS;
  - (b) the introduction of significant risk into CECS.
- (2) If the affected parties decide that they have enough information to make a recommendation, Payments NZ must—
  - (a) ensure that the affected parties complete the device compromise submission specified in appendix 22B no later than 48 hours after any of the following occur in respect to the model of device—
    - (i) Payments NZ receives notification under clause 4.2(1); or
    - (ii) Payments NZ makes a decision under clause 4.3(1)(b); and
  - (b) as soon as practicable after receiving the submission, send a copy of the submission to the CECS management committee and to the board.
- (3) If the affected parties decide that they do not have enough information to make a recommendation, Payments NZ must—
  - (a) ensure that the affected parties complete as much as practicable of the device compromise submission no later than 48 hours after any of the following occur in respect to the model of device—
    - (i) Payments NZ receives notification under clause 4.2(1); or
    - (ii) Payments NZ makes a decision under clause 4.3(1)(b); and
  - (b) as soon as practicable after receiving the incomplete submission, send a copy to the CECS management committee and to the board; and
  - (c) require the affected parties to complete the device compromise submission including the recommendation as soon as practicable; and
  - (d) as soon as practicable after receiving the complete submission, send a copy to the CECS management committee and to the board.

This appendix 22B specifies the content required and the format of the device compromise submission.

### Table of contents

<a href="#">1. Compromised device incident</a>	41
<a href="#">2. Compromised device</a>	42
<a href="#">3. Compromise details</a>	43
<a href="#">4. Removing devices</a>	44
<a href="#">5. Merchants</a>	45
<a href="#">6. Potential payment instrument fraud</a>	47
<a href="#">7. Investigations</a>	48
<a href="#">8. Potential device removal impact assessment</a>	54
<a href="#">9. Prevention</a>	55
<a href="#">10. Risk analysis and recommendation</a>	56



## 1. Compromised device incident

The acquirer who acquires EFTPOS transactions from the compromised device must complete the following:

**Date acquirer became aware of the compromise:**

From:

Click here to enter a date.

To:

Click here to enter a date.

**Number of devices compromised:**

Click here to enter text.

Final no.

On-going no.

**Number of merchants affected:**

Click here to enter text.

Final no.

On-going no.

**Number of merchant locations:**

Click here to enter text.

Final no.

On-going no.

**Names of acquirers who acquire transactions from the compromised model:**

Click here to enter text.

**Level of severity:**

Minor

Medium

Major

**Reasons for the level of severity selected:**

**Any more relevant information about the compromise:**

## 2. Compromised device

The acquirer who acquires transactions from the compromised device must complete the following:

On Payments NZ device register?  Yes  No

Manufacturer:  Model:

Product type:

Standalone  Integrated

Attended  Unattended

Payments NZ sunset date:

Payments NZ date of no new connections:

Included on the PCI certification list?  Yes  No

PCI version no.:

Software version:

Revision number:

Number of devices in the market:

Date device first connected to the EFTPOS switching network:

Is there any known overseas compromise activity on this model of device?  Yes  No

If yes, provide details:

Any more relevant information on the model of compromised device:

### 3. Compromise details

The acquirer who acquires transactions from the compromised device must complete the following:

**What type of data was compromised:**

- EMV data       Magstripe data       PIN

**Type of intervention:**

- Hardware       Software

**How was the device tampered with?**

- Physical/in-store       Remotely

**How was the device accessed to initiate the compromise?**

**Were anti-tamper detection mechanisms triggered?**

- Yes       No

**Were any of the following attached to the device?**

- Magstripe skimmer       PIN skimmer       Other (*please specify*)

**Complexity of compromise:**

- Not complex       Slightly       Reasonably       Very

**Any more relevant information on the compromise:**

## 4. Removing devices

The acquirer who acquires transactions from the compromised device must complete the following:

Have the devices been removed from the site/s?

No

Some

All

If no or some, why?

If no or some, when will the device/s be removed from the site?

[Click here to enter a date.](#)

Any more relevant information on the removal:

## 5. Merchants

The acquirer who acquires transactions from the compromised device must complete the following:

### 5a. Merchants affected by the device compromise

	No. of merchants	No. of devices	No. of locations
<input type="checkbox"/> Small merchant:	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>
<input type="checkbox"/> Medium merchant:	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>
<input type="checkbox"/> Large merchant:	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>	<input type="text" value="Click here to enter text."/>

Which sectors do the merchants operate in?

Identify the 10 largest merchants affected by the device compromise.

1.	<input type="text" value="Click here to enter text."/>
2.	<input type="text" value="Click here to enter text."/>
3.	<input type="text" value="Click here to enter text."/>
4.	<input type="text" value="Click here to enter text."/>
5.	<input type="text" value="Click here to enter text."/>
6.	<input type="text" value="Click here to enter text."/>
7.	<input type="text" value="Click here to enter text."/>
8.	<input type="text" value="Click here to enter text."/>
9.	<input type="text" value="Click here to enter text."/>
10.	<input type="text" value="Click here to enter text."/>

### 5b. Merchants using the model of device not affected by the compromise

	No. of merchants	No. of devices	No. of locations
<input type="checkbox"/> Small merchant:	Click here to enter text.	Click here to enter text.	Click here to enter text.
<input type="checkbox"/> Medium merchant:	Click here to enter text.	Click here to enter text.	Click here to enter text.
<input type="checkbox"/> Large merchant:	Click here to enter text.	Click here to enter text.	Click here to enter text.

**Which sectors do the merchants operate in?**

**Identify the 10 largest merchants using the model of device not affected by the device compromise.**

1.	Click here to enter text.
2.	Click here to enter text.
3.	Click here to enter text.
4.	Click here to enter text.
5.	Click here to enter text.
6.	Click here to enter text.
7.	Click here to enter text.
8.	Click here to enter text.
9.	Click here to enter text.
10.	Click here to enter text.

## 6. Potential payment instrument fraud

The acquirer who acquires transactions from the compromised device must complete the following:

Have any common points of purchase been identified?

Yes

No

Number of cards at risk of being compromised:

Click here to enter text.

Number of payment applications on mobile devices at risk of being compromised:

Click here to enter text.

Any more relevant information about payment instrument fraud

## 7. Investigations

The acquirer who acquires transactions from the compromised device must complete the following:

**Identify which of the following reports are being completed?**

- Scheme preliminary forensic       Scheme final forensic       Police report  
 Independent consultancy report       Other (*please specify*)

Click here to enter text.

**Identify which of the following reports are already available?**

- Scheme preliminary forensic       Scheme final forensic       Police report  
 Independent consultancy report       Other (*please specify*)

Click here to enter text.

**Specify when the reports not yet provided will be available?**

Name of the report:

Will be available on:

Click here to enter text.

Click here to enter a date.

Click here to enter text.

Click here to enter a date.

Click here to enter text.

Click here to enter a date.

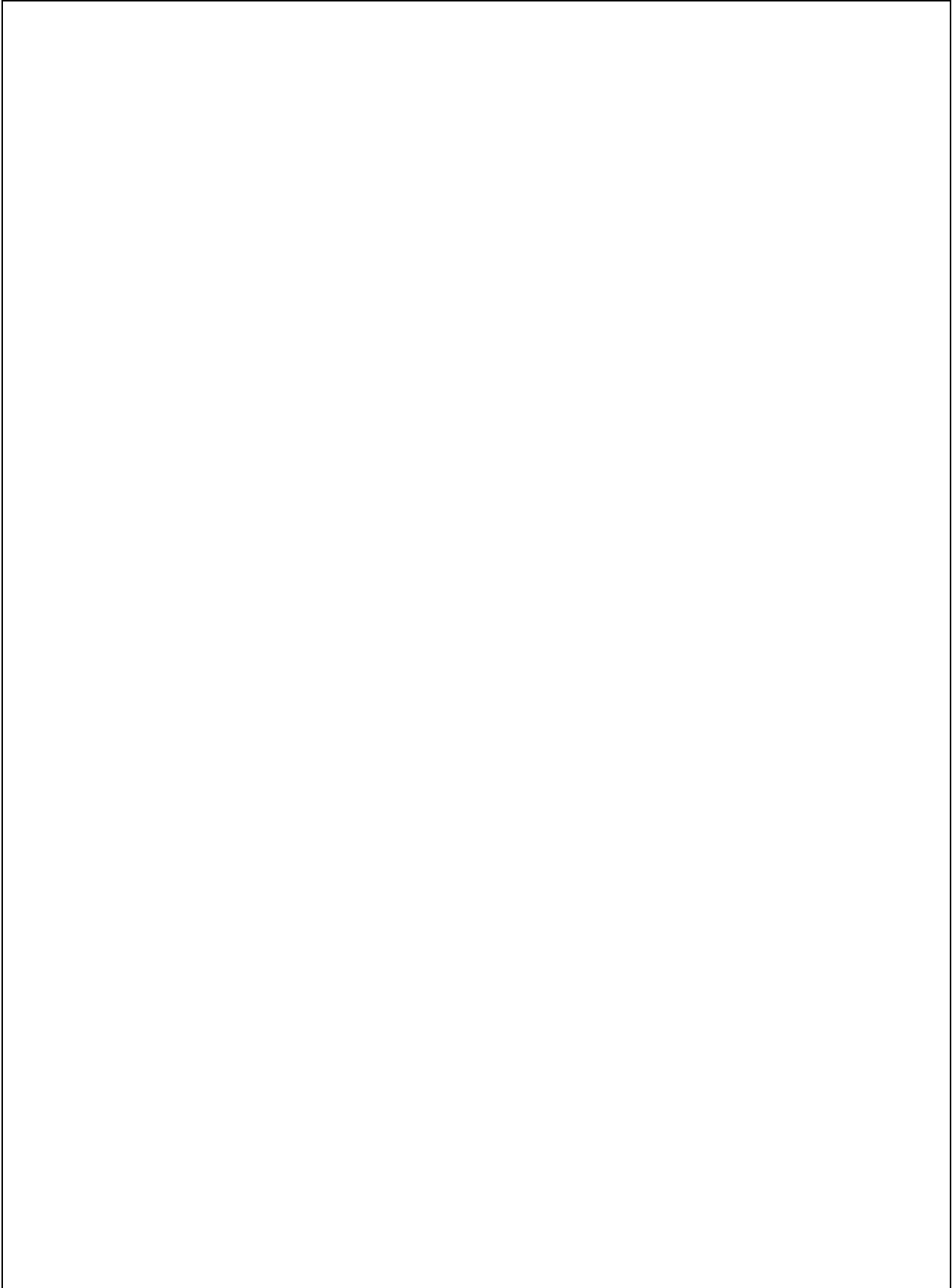
**Any more relevant information about the availability of the reports:**



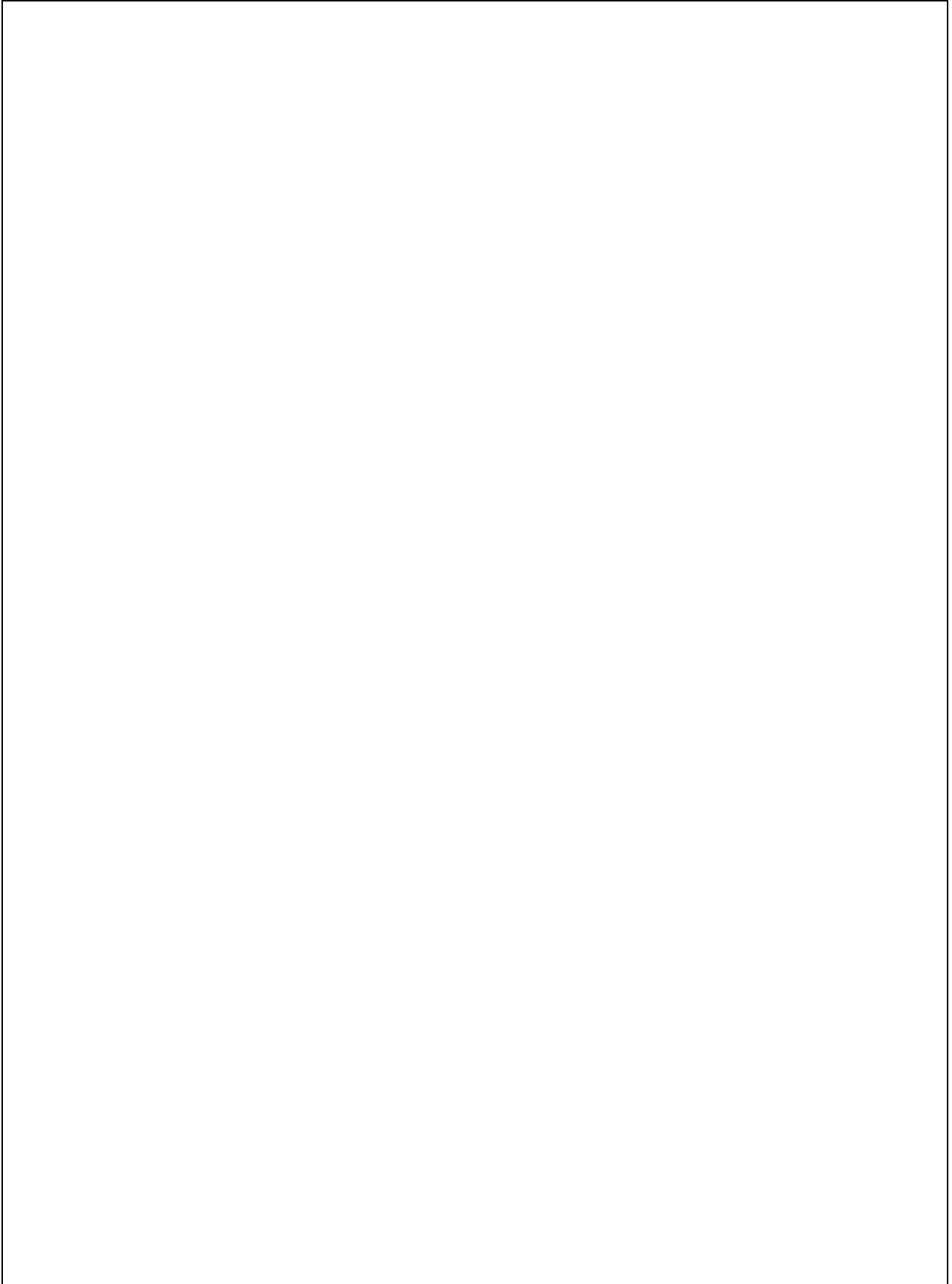
Specify the details of the main conclusions and findings for the reports that are available:

**Scheme preliminary forensic report**

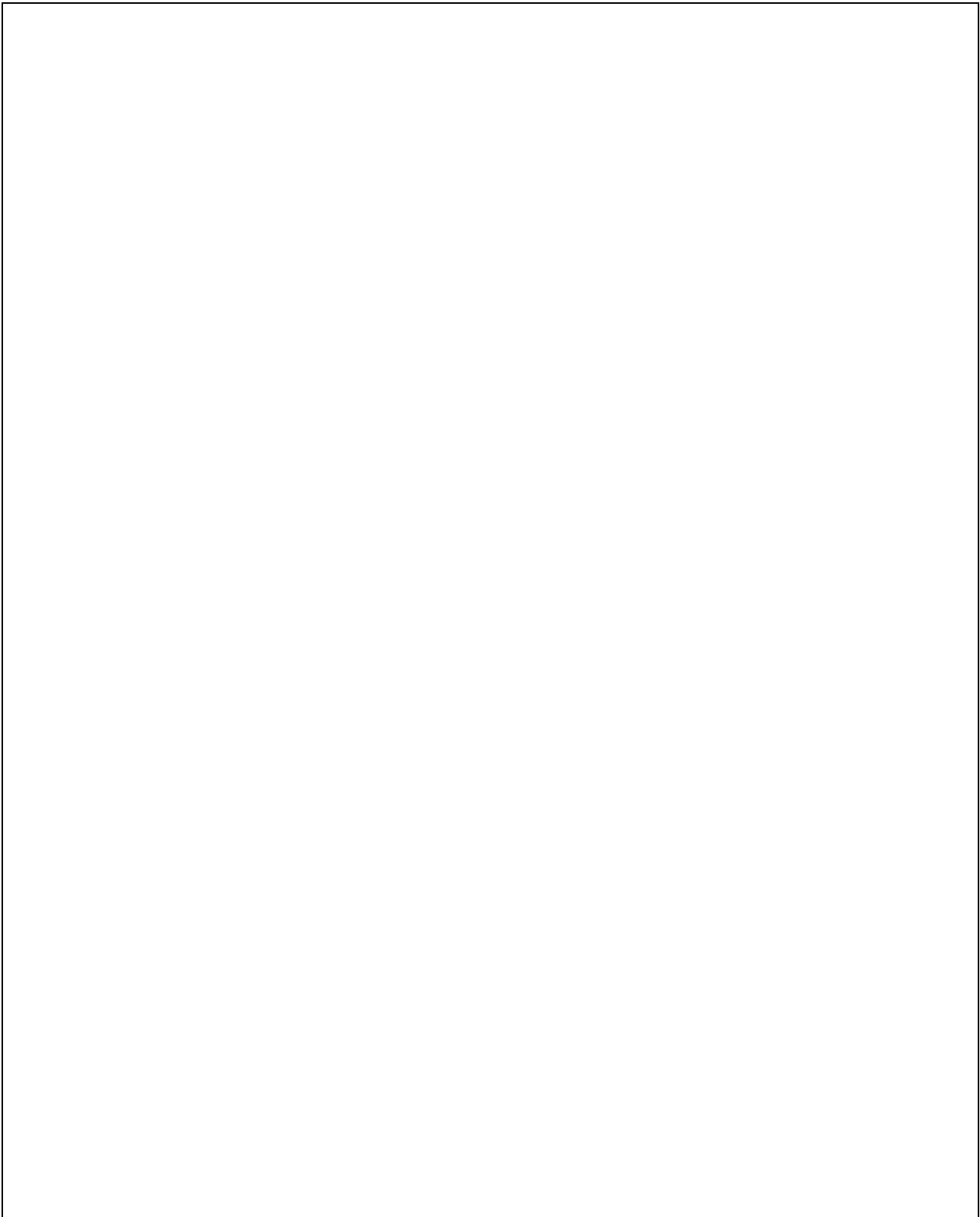
**Scheme final forensic report**



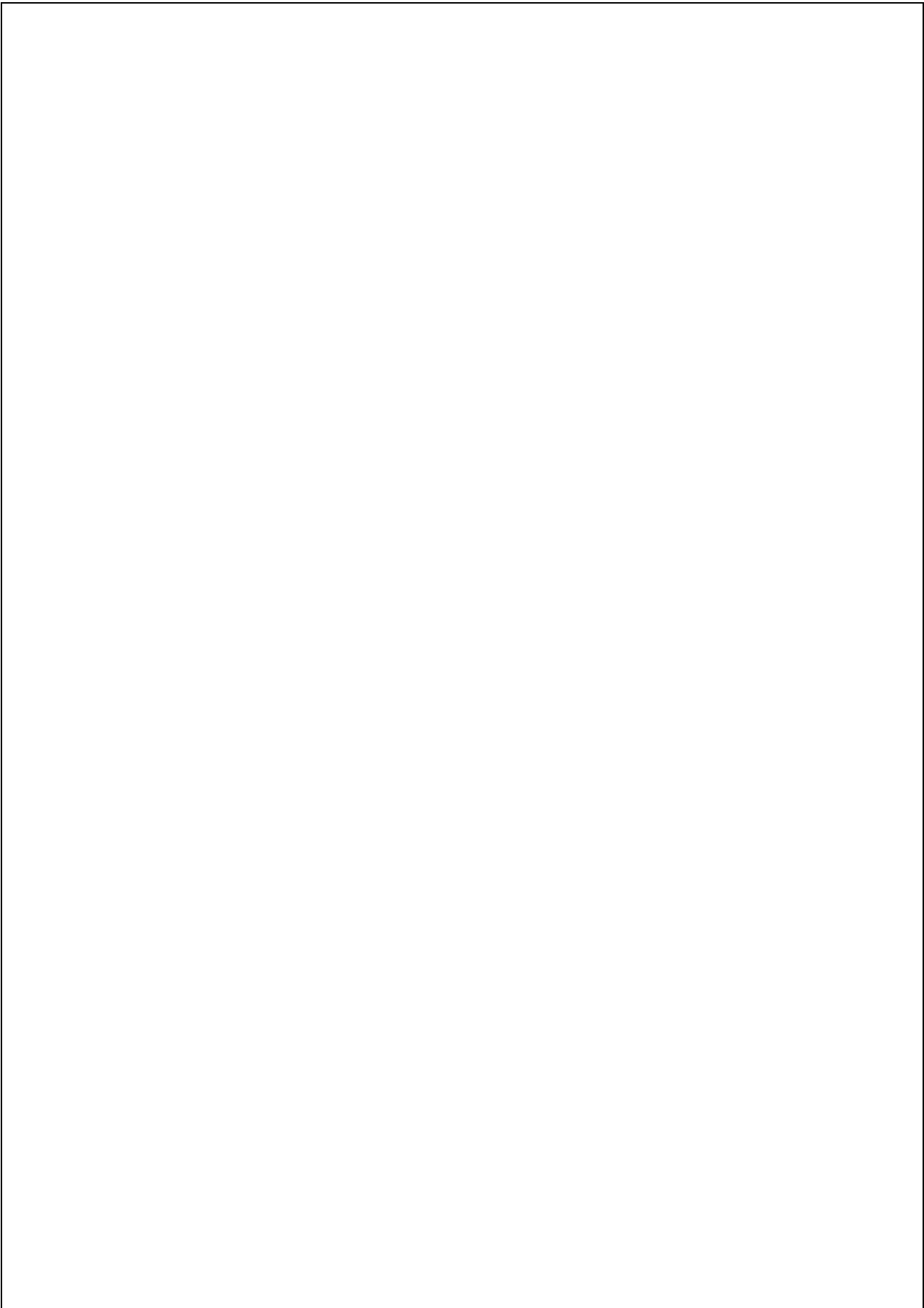
## Police report

A large, empty rectangular box with a thin black border, occupying most of the page. It is intended for a police report.

## Independent consultancy report



**Other reports available**



## 8. Potential device removal impact assessment

The acquirer who acquires transactions from the compromised device must complete the following in respect of the proposed replacement model of device:

Is the replacement model on Payments NZ device register?

Yes  No

Replacement model manufacturer:

Click here to enter text.

Replacement model:

Click here to enter text.

Replacement model sunset date:

Click here to enter a date.

Replacement model date of no new connections:

Click here to enter a date.

Replacement model PCI version no.:

Click here to enter text.

Replacement model software version:

Click here to enter text.

Replacement model revision number:

Click here to enter text.

Included on PCI certification list?

Click here to enter text.

Number of devices in the market of the replacement model:

Click here to enter text.

**Multiple devices** (Provide details above of the device planned for the highest volume of placements)

What development is required on device before being placed in the market?

Hardware

Software

Switch certification

Scheme certification

Other (please specify)

Click here to enter text.

Please provide more information on development required here:

What is the estimated removal replacement timeline?

Start:

Click here to enter a date.

Finish:

Click here to enter a date.

Give the reasons for the estimated timeline for replacement (e.g. time needed to deliver functional gaps between the devices) and any other relevant information on stock availability:

## 9. Prevention

The acquirer who acquires transactions from the compromised device must complete the following with the help of others in the group:

**Specify the steps undertaken or planned to prevent a compromise from re-occurring?**

**If steps are planned to prevent a compromise from re-occurring, when will they take place?**

## 10. Risk analysis and recommendation

All affected parties must complete the following:

Has another compromise occurred since remediation?  Yes  No  Not yet able to answer

If yes, provide details:

Based on the information in this submission, indicate the level of risk to the market for each of the following 2 scenarios?

1. Require disconnection of the model of device from the EFTPOS switching network.  Low  Medium  High

Give the reasons for the level of risk indicated:

2. Allow for the device to remain connected to the EFTPOS switching network and take steps to prevent re-occurrence of the compromise described in section 9 above.  Low  Medium  High

Give the reasons for the level of risk indicated:



**Based on the level of risk indicated, provide your recommendation for whether or not the model of device should be disconnected from the EFTPOS switching network:**

**Disconnect the model of device**

Recommended date to disconnect the model of device from the switching network:

Click here to enter a date.

Recommended date from which devices of the model of device must not connect for the first time to the EFTPOS switching network:

Click here to enter a date.

**Give the reasons for your recommendations including the recommended dates:**

**Do not disconnect the device**

**Give the reasons for your recommendation:**

**Recommended steps to prevent another compromise:**

**More time is needed to make a recommendation**

Why is more time needed to make a recommendation?

When will a recommendation be made:

Click here to enter a date.

## Appendix 22C: Compromised device disconnection plan

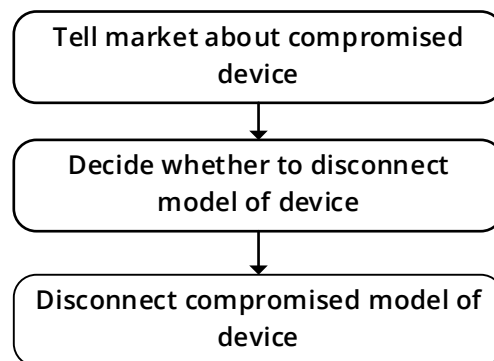
---

### Purpose

This plan describes a 3-stage process specified in chapter 5 of the Payments NZ EFTPOS device life cycle standards for disconnecting a model of device from the EFTPOS switching network if—

- the device fails to protect sensitive data on a payment instrument from unauthorised disclosure or use in New Zealand or overseas; and
- the failure is the result of 1 or more attributes of the model of device.

The following diagram shows at a high level the stages in the process—



The purpose of the plan is to help—

- manage disconnection of a compromised device quickly and efficiently; and
- include stakeholders who are not Payments NZ participants in the process; and
- ensure effective oversight of the process; and
- enable affected stakeholders to focus on resolving the issue; and
- minimise the effect of the compromise on merchants and their customers.

The plan has no legal effect. The Payments NZ rules and standards bind participants and Payments NZ but no other entities (e.g. switches). If the Payments NZ rules or standards and the plan are inconsistent, the rules or standards apply to Payments NZ and participants.

The terms and conditions between Payments NZ and the device vendor who has applied for registration of the compromised device on the Payments NZ device register, bind the device vendor. If the terms and conditions and the plan are inconsistent, the terms and conditions apply to Payments NZ and the device vendor.

---

**People involved in the process**

The following table describes those affected by the 3-stage process—

<b>Person</b>	<b>Description</b>
<b>Acquirer</b>	Payments NZ participant who acquires EFTPOS transactions from a merchant's device.
<b>Board</b>	Payments NZ's board of directors.
<b>CECS management committee</b>	Payments NZ's management committee responsible for the consumer electronic clearing system.
<b>Issuer</b>	Payments NZ participant who issues cards or payment applications on mobile devices.
<b>Merchant</b>	A supplier of goods or services who uses a device to receive payments from customers who use cards or payment applications on mobile devices to interact with the device.
<b>Payments NZ</b>	A company that regulates connection of models of devices to the EFTPOS switching network. Only models of device that are registered on Payments NZ's device register can connect to the network.
<b>Switch company</b>	A company that connects devices to the EFTPOS switching network. The network delivers payment instructions from merchants' devices to issuers for authorisation.
<b>Device reseller</b>	A person who sells or leases a device to a merchant.
<b>Device vendor</b>	A person who creates a model of device and applies to Payments NZ for registration of the model.

**Contents**

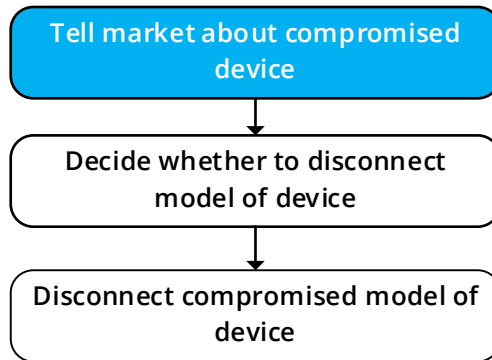
The plan describes the process in the following sections:

<b>Section</b>	<b>See page</b>
Section A: Communicating a compromise	60
Section B: Decision to disconnect	62
Section C: Disconnection process	68

## Section A: Communicating a compromise

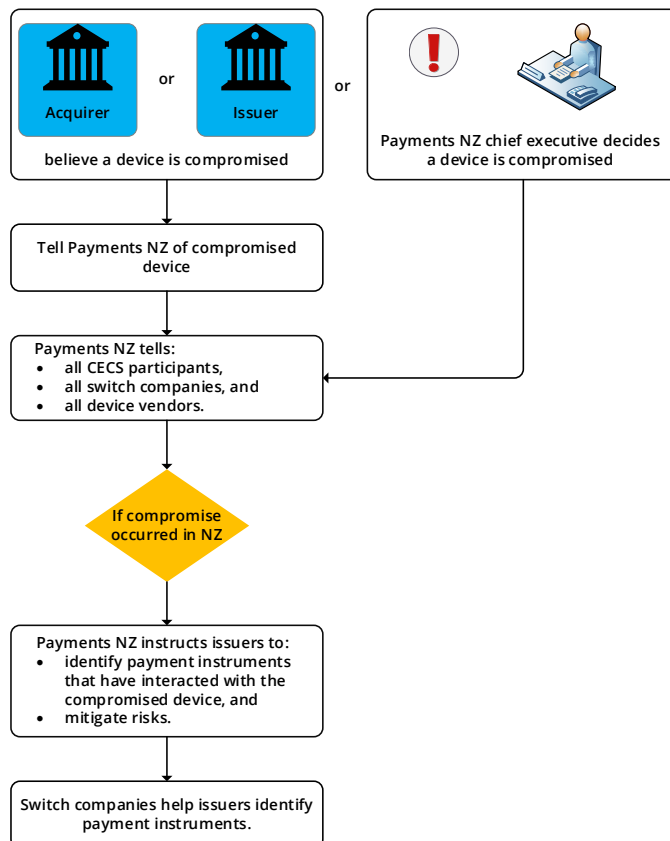
### 1st stage

During the 1st stage in the Payments NZ compromised device disconnection process, acquirers, issuers, Payments NZ, switches and device vendors communicate with each other about the failure of a device to protect sensitive data on a payment instrument. The highlighted block in the following diagram shows the stage in the process described in this section.



### Process overview

The following diagram gives a high-level view of the 1st stage in the process—



**Roles and responsibilities**

The following table summarises the roles and responsibilities of those involved in the 1st stage of the process—

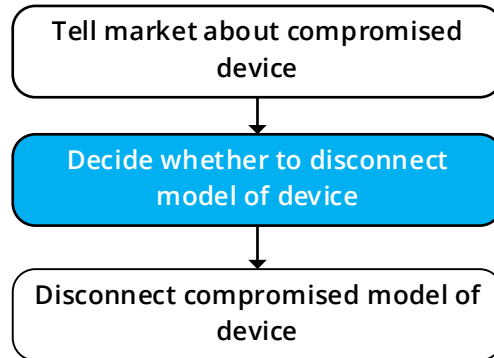
Person	Description
<b>Acquirer</b>	<ul style="list-style-type: none"> <li>• If acquirer believes a device has failed to protect sensitive data on a card or a payment application on a mobile device, notify Payments NZ.</li> <li>• Require its switch to help issuers identify payment instruments that have interacted with the compromised device.</li> </ul>
<b>Issuer</b>	<ul style="list-style-type: none"> <li>• If an issuer believes a device has failed to protect sensitive data on a card or a payment application on a mobile device, notify Payments NZ.</li> <li>• Identify every card or payment application on a mobile device issued by the issuer that has interacted with the device.</li> <li>• Determine whether to take any steps to prevent—               <ul style="list-style-type: none"> <li>– an adverse effect on the integrity or the reputation of CECS; or</li> <li>– the introduction of significant risk into CECS (e.g. notifying a card holder of the interaction with the device or cancelling the card).</li> </ul> </li> </ul>
<b>Payments NZ</b>	<ul style="list-style-type: none"> <li>• Receives notifications of a device's failure to protect sensitive data or decides a device has failed to protect sensitive data for any other reason.</li> <li>• Notifies participants, switches, and device vendors of the failure to protect sensitive data on a card or a payment application on a mobile device.</li> <li>• Instructs issuers to—               <ul style="list-style-type: none"> <li>– identify each payment instrument issued that has interacted with the device; and</li> <li>– determine whether to take any steps to prevent—                   <ul style="list-style-type: none"> <li>○ an adverse effect on the integrity or the reputation of CECS; or</li> <li>○ the introduction of significant risk into CECS (e.g. notifying a card holder of the interaction with the device or cancelling the card).</li> </ul> </li> </ul> </li> <li>• Instructs the acquirer who acquires transactions from the device to require its switch to help issuers identify cards or payment applications on mobile devices that have interacted with the device.</li> <li>• Communicates with media about the device compromise.</li> </ul>
<b>Switch</b>	<p>If requested by an issuer, help the issuer to identify payment instruments issued by the issuer that have interacted with the device.</p>

## Section B: Decision to disconnect

---

### 2nd stage

The highlighted block in the following diagram shows the 2nd stage in the compromised device disconnection process that is described in this section—



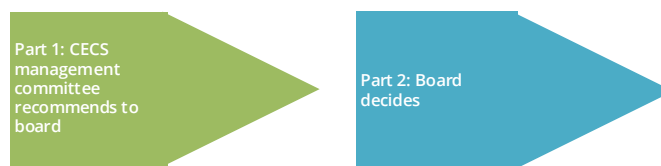
For a device compromise in New Zealand, during the 2nd stage in the process—

- acquirers, switches, issuers and the device vendor have 48 hours to recommend to Payments NZ whether to disconnect the compromised model of device from the EFTPOS switching network; and
- Payments NZ (via the CECS management committee and the board) has another 48 hours to decide whether to disconnect.

The decision process is split into the following 3 parts:



For a device compromise overseas, during the 2<sup>nd</sup> stage in the process, the CECS management committee and the board determine whether to disconnect the model of device at the next scheduled meetings of the committee and the board.



### Contents

This section describes the following topics:

Topic	See page
B1: NZ compromise: affected parties recommend	63
B2: Management committee recommends and board decides	66

---

# B1: NZ compromise: affected parties recommend

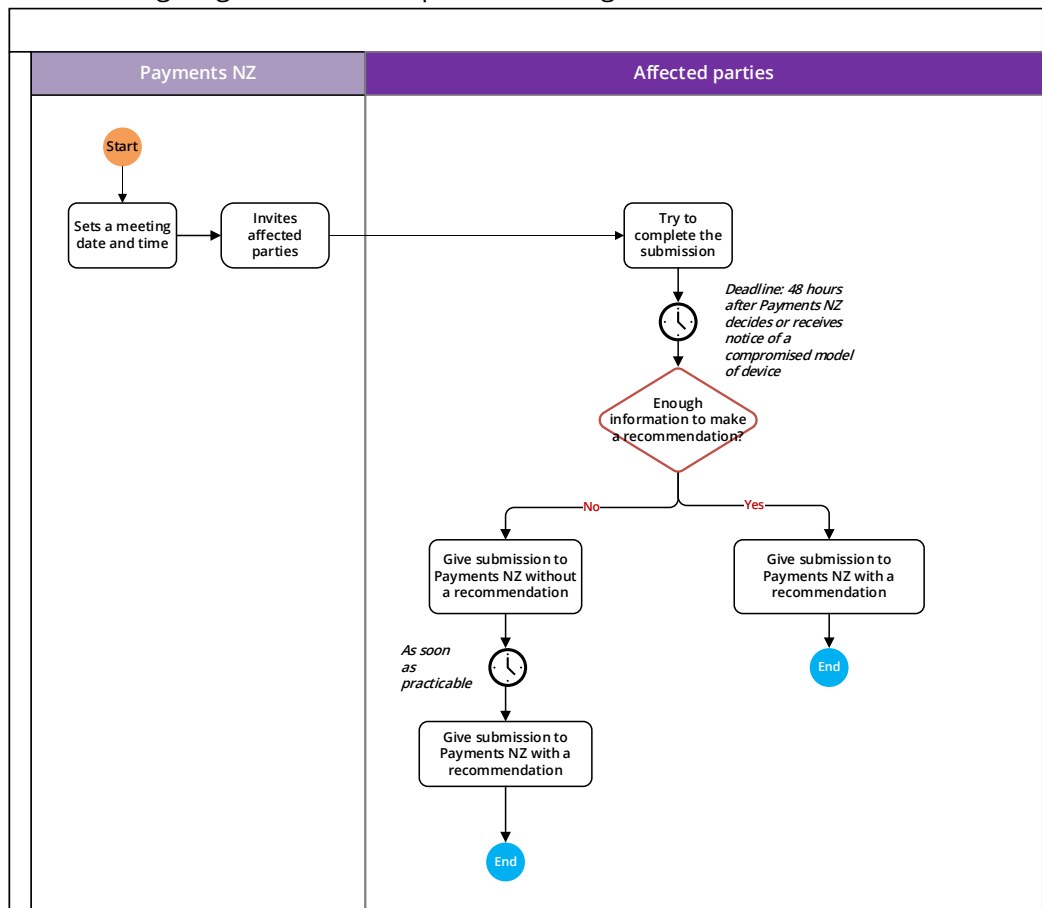
## Process overview

For a device compromise in New Zealand, during the 1st part of the decision process the Payments NZ chief executive, the device vendor, switches, and acquirers who connect devices of the model to the switching network, issuers whose payment instruments have interacted with the compromised device and other experts—

- review the causes and consequences of the device’s failure to protect sensitive data on a payment instrument; and
- recommend to Payments NZ whether to disconnect the model of device from the switching network.

The affected parties put the information and the recommendation in a submission for the Payments NZ CECS management committee and the Payments NZ board to consider. The affected parties have 48 hours to try to complete a submission containing a recommendation.

The following diagram shows the process at a high level:



**Payments NZ  
arranges  
meeting to  
complete  
submission**

To arrange a meeting of affected parties, the Payments NZ chief executive—

#	Action
1	<ul style="list-style-type: none"> <li>• invites the those specified on the compromised device contact list for—               <ul style="list-style-type: none"> <li>– the device vendor who applied for registration of the model of device on the Payments NZ device register; and</li> <li>– every switch company that connects devices of the model to the EFTPOS switching network; and</li> <li>– every acquirer who connects devices of the model to the EFTPOS switching network; and</li> <li>– every issuer who issued a payment instrument that interacted with the compromised device; and</li> </ul> </li> <li>• for each representative invited, uses the email address specified on the compromised device contact list.</li> </ul>
2	<ul style="list-style-type: none"> <li>• may use the notice specified in device form 3 to invite the affected parties to the meeting; and</li> <li>• may attach the following to the notice—               <ul style="list-style-type: none"> <li>– the agenda specified in compromise device form 4; and</li> <li>– the submission template specified in appendix 22C.</li> </ul> </li> </ul>

**Affected  
parties’  
meeting**

At the meeting of affected parties—

#	Action						
1	<p>The affected parties decide whether they have enough information to recommend to the CECS management committee and the board whether to disconnect the model of device to prevent—</p> <ul style="list-style-type: none"> <li>• an adverse effect on the integrity or the reputation of CECS; or</li> <li>• introduction of significant risk into CECS.</li> </ul> <p>The affected parties decide within 48 hours of the Payments NZ chief executive receiving notice of the compromise or deciding that a compromise has occurred.</p>						
2	<table border="1"> <thead> <tr> <th>If the affected parties decide...</th> <th>then...</th> </tr> </thead> <tbody> <tr> <td>the affected parties can make a recommendation within the 48-hour deadline,</td> <td> <ul style="list-style-type: none"> <li>• the affected parties complete the submission and include the recommendation; and</li> <li>• the Payments NZ chief executive arranges meetings of the CECS management committee and the board and sends them the submission.</li> </ul> </td> </tr> <tr> <td>the affected parties do not have enough information to make a recommendation within the 48-hour deadline,</td> <td> <ul style="list-style-type: none"> <li>• the affected parties complete as much of the submission as practicable without including a recommendation, and</li> <li>• the Payments NZ chief executive:               <ul style="list-style-type: none"> <li>– sends the incomplete submission to the CECS management committee and the board; and,</li> <li>– requires the affected parties to make a recommendation as soon as practicable; and</li> <li>– arranges meetings of the management committee and the board when the affected parties make a recommendation.</li> </ul> </li> </ul> </td> </tr> </tbody> </table>	If the affected parties decide...	then...	the affected parties can make a recommendation within the 48-hour deadline,	<ul style="list-style-type: none"> <li>• the affected parties complete the submission and include the recommendation; and</li> <li>• the Payments NZ chief executive arranges meetings of the CECS management committee and the board and sends them the submission.</li> </ul>	the affected parties do not have enough information to make a recommendation within the 48-hour deadline,	<ul style="list-style-type: none"> <li>• the affected parties complete as much of the submission as practicable without including a recommendation, and</li> <li>• the Payments NZ chief executive:               <ul style="list-style-type: none"> <li>– sends the incomplete submission to the CECS management committee and the board; and,</li> <li>– requires the affected parties to make a recommendation as soon as practicable; and</li> <li>– arranges meetings of the management committee and the board when the affected parties make a recommendation.</li> </ul> </li> </ul>
If the affected parties decide...	then...						
the affected parties can make a recommendation within the 48-hour deadline,	<ul style="list-style-type: none"> <li>• the affected parties complete the submission and include the recommendation; and</li> <li>• the Payments NZ chief executive arranges meetings of the CECS management committee and the board and sends them the submission.</li> </ul>						
the affected parties do not have enough information to make a recommendation within the 48-hour deadline,	<ul style="list-style-type: none"> <li>• the affected parties complete as much of the submission as practicable without including a recommendation, and</li> <li>• the Payments NZ chief executive:               <ul style="list-style-type: none"> <li>– sends the incomplete submission to the CECS management committee and the board; and,</li> <li>– requires the affected parties to make a recommendation as soon as practicable; and</li> <li>– arranges meetings of the management committee and the board when the affected parties make a recommendation.</li> </ul> </li> </ul>						



**Roles and responsibilities**

The following table summarises the roles and responsibilities of those involved in the process of completing the device compromise submission—

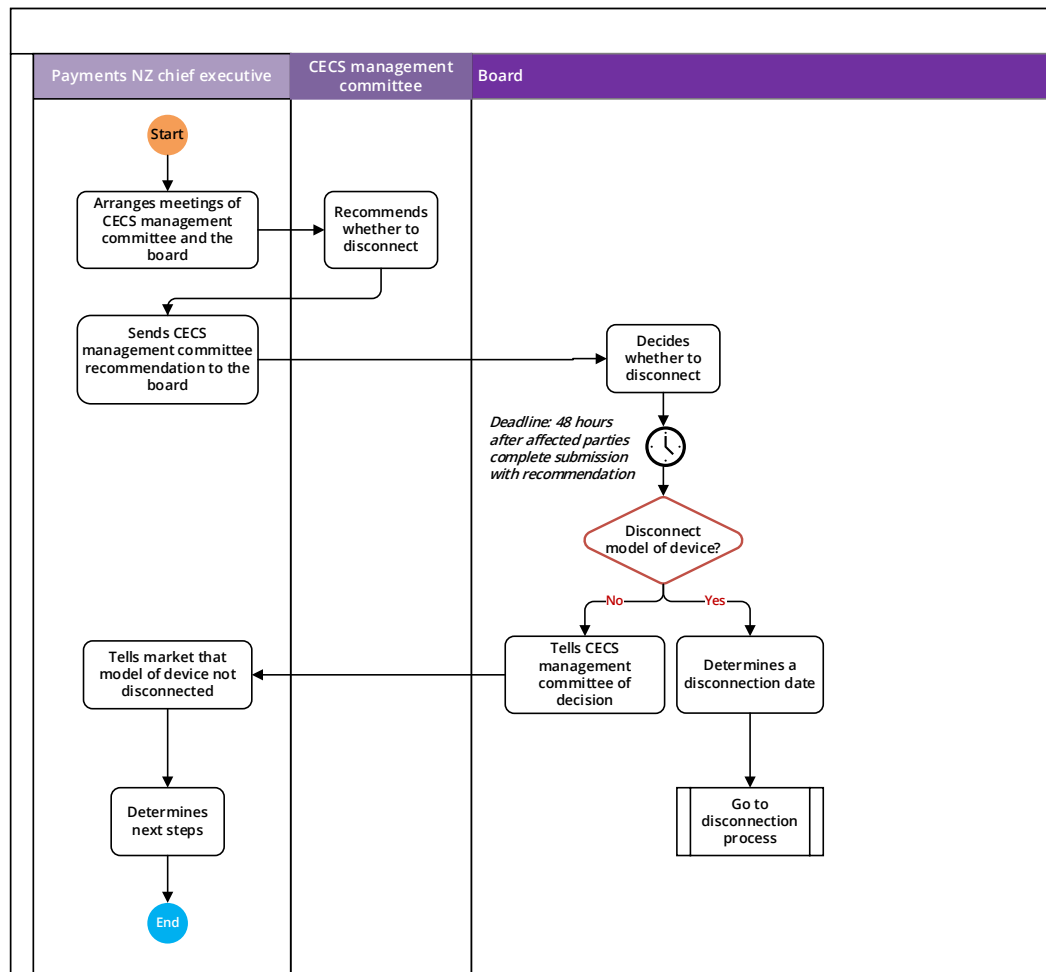
Person	Roles and responsibilities
<b>Acquirer</b>	<p>If an acquirer is invited to the meeting of affected parties—</p> <ul style="list-style-type: none"> <li>• attend the meeting; and</li> <li>• try to provide the information that Payments NZ requires for the device compromise submission as soon as practicable after Payments NZ requests the information; and</li> <li>• arrange any reports required by Payments NZ in respect of the device compromised or the merchant operating the device, for example, a forensic report or a police report; and</li> <li>• provide Payments NZ with the details that Payments NZ requires of the reports; and</li> <li>• during the period in which the affected parties complete the device compromise submission, monitor the market to determine whether any other device connected to the EFTPOS switching network fails to protect sensitive data on a payment instrument; and</li> <li>• help Payments NZ to coordinate and lead meetings of the affected parties.</li> </ul>
<b>Issuer</b>	<p>If an issuer is invited to the meeting of affected parties—</p> <ul style="list-style-type: none"> <li>• attend the meeting; and</li> <li>• try to provide any information that Payments NZ requires for the device compromise submission as soon as practicable after Payments NZ requests the information from the issuer.</li> </ul>
<b>Payments NZ chief executive</b>	<ul style="list-style-type: none"> <li>• Arranges the meeting of affected parties.</li> <li>• Leads and attends the meetings.</li> <li>• Records the decisions of the affected parties in the device compromise submission.</li> <li>• Updates the CECS management committee and the Payments NZ board on— <ul style="list-style-type: none"> <li>– the affected parties’ progress towards completing the submission; and</li> <li>– when the committee and the board may be required to decide whether to disconnect the model of device.</li> </ul> </li> <li>• Communicates with media about the device compromise.</li> </ul>
<b>Switch</b>	<p>If a switch is invited to the meeting of affected parties—</p> <ul style="list-style-type: none"> <li>• attend the meeting; and</li> <li>• try to provide any information that Payments NZ requires for the device compromise submission as soon as practicable after Payments NZ requests the information from the switch.</li> </ul>
<b>Device vendor</b>	<p>If a device vendor is invited to the meeting of affected parties—</p> <ul style="list-style-type: none"> <li>• attend the meeting; and</li> <li>• try to provide any information that Payments NZ requires for the device compromise submission as soon as practicable after Payments NZ requests the information from the device vendor.</li> </ul>

## B2: Management committee recommends and board decides

### Overview of process

The following diagram summarises the process in which—

- the CECS management committee meets and recommends to the board whether or not to disconnect the compromised model of device from the EFTPOS switching network; and
- the board decides whether or not to disconnect the compromised model of device from the EFTPOS switching network and, if it requires disconnection, a disconnection date and a date from which devices of the model cannot connect for the first time to the EFTPOS switching network.



---

**Roles and responsibilities**

The following table summarises the roles and responsibilities of those involved in the decisions of the CECS management committee and the board—

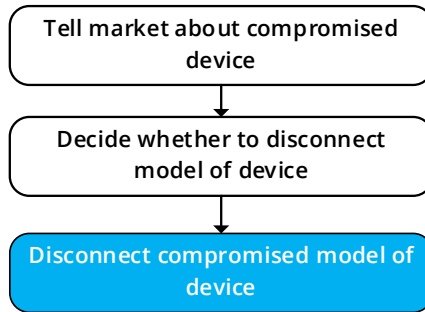
<b>Person</b>	<b>Roles and responsibilities</b>
<b>Acquirer</b>	Make submissions to the committee or to the board.
<b>Issuer</b>	Make submissions to the committee or to the board.
<b>Payments NZ</b>	Communicates with media about the device compromise.
<b>Switch</b>	Make submissions to the committee or to the board.
<b>Device vendor</b>	Make submissions to the committee or to the board.

---

## Section C: Disconnection process

### 3rd stage

The highlighted block in the following diagram shows the 3<sup>rd</sup> stage in the compromised device disconnection process described in this section—

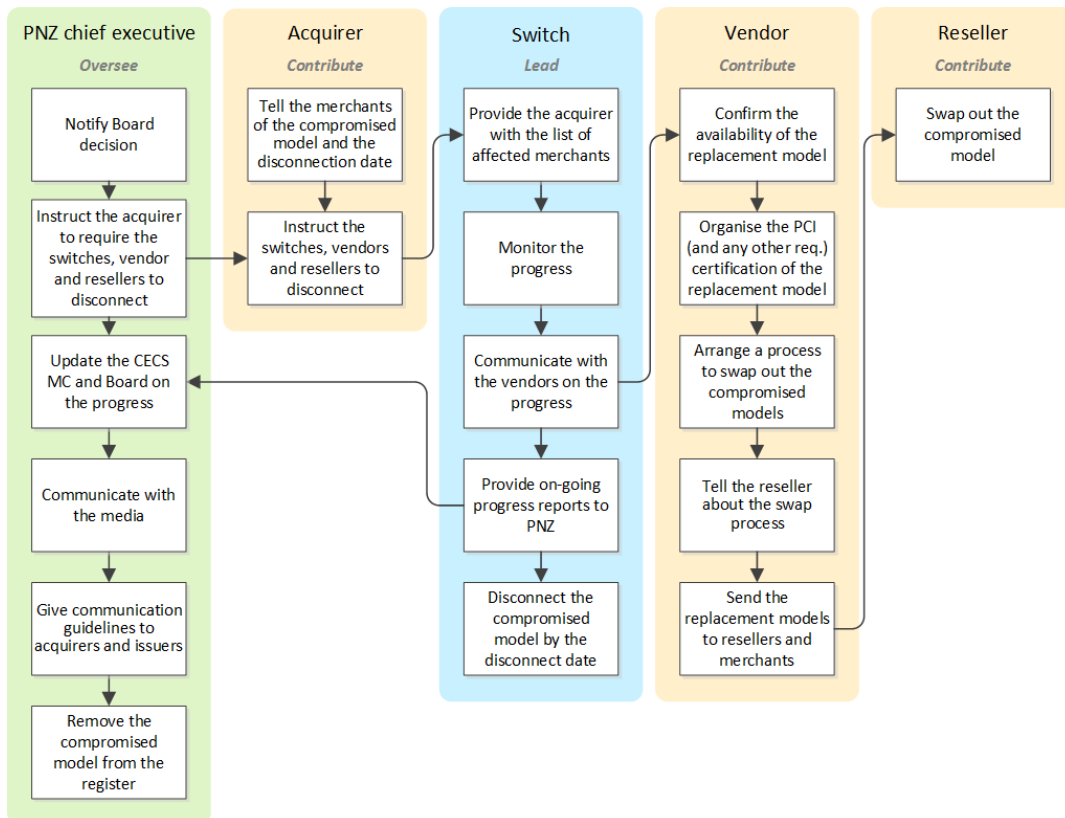


If the Payments NZ board requires disconnection of a compromised model of device from the switching network, during the 3<sup>rd</sup> stage in the process the following work together to disconnect it and replace it with a different model:

- acquirers:
- Payments NZ:
- switches:
- device resellers:
- the device vendor.

### Overview of roles

The following drawing gives a high-level overview of the roles and responsibilities of those involved in the disconnection process—



**Roles and responsibilities**

The following table describes in more detail the roles and responsibilities of those involved in the disconnection process—

Person	Role and responsibility
<b>Acquirer</b>	<ul style="list-style-type: none"> <li>• Tell merchants who operate the compromised model of device of the board’s decision to disconnect the model of device, the disconnection date and that the merchant will require a replacement device of a different model no later than the disconnection date.</li> <li>• Comply with Payments NZ’s instructions by requiring switches, the device vendor and device resellers to take the steps specified by the Payments NZ EFTPOS device life cycle standards to disconnect and replace the compromised model of device.</li> </ul>
<b>Payments NZ</b>	<ul style="list-style-type: none"> <li>• Using compromised device form 2,—               <ul style="list-style-type: none"> <li>– notifies participants, switches and device vendors of the board’s decision and the disconnection date; and</li> <li>– instructs acquirers to require switches, the device vendor and device resellers to take the steps specified by the Payments NZ EFTPOS device life cycle standards to disconnect and replace the compromised model of device.</li> </ul> </li> <li>• Communicates with media about the device compromise and the disconnection process.</li> <li>• Gives guidelines to—               <ul style="list-style-type: none"> <li>– acquirers for communicating with media and merchants about the compromise and the disconnection process; and</li> <li>– issuers for communicating with media and customers about the compromise and the disconnection process.</li> </ul> </li> </ul>
<b>Switch company</b>	<p>Comply with acquirers’ instructions to—</p> <ul style="list-style-type: none"> <li>• tell acquirers the names of merchants operating the compromised model of device; and</li> <li>• manage and monitor the disconnection and replacement process; and</li> <li>• manage communications with the device vendor about the disconnection and replacement process; and</li> <li>• during the disconnection and replacement process, tell Payments NZ when Payments NZ requires of the number of devices disconnected and replaced; and</li> <li>• on the no new connections date, prevent devices of the compromised from connecting for the first time to the EFTPOS switching network; and</li> <li>• by the disconnection date, disconnect the compromised model of device.</li> </ul>
<b>Device reseller</b>	<p>Comply with a device vendor’s instructions to replace the compromised model of device with the replacement model of device.</p>
<b>Device vendor</b>	<p>Comply with a switch company’s instructions to—</p> <ul style="list-style-type: none"> <li>• determine the number of devices of the compromised model to be disconnected and replaced with a different model of device; and</li> <li>• confirm whether the vendor can replace every device of the compromised model with a different model of device by the disconnection date; and</li> <li>• determine any functional differences between the compromised model of device and the replacement model of device and ensure that the replacement model of equal functionality at least; and</li> <li>• if the replacement model of device is not registered on the Payments NZ device register, apply to Payments NZ to register the model of device; and</li> <li>• if the replacement model of device requires approval from any other entity (e.g. a switch) before connection to the EFTPOS switching network, arrange to get the approval; and</li> <li>• arrange a process to disconnect devices of the compromised model and replace them with devices of the replacement model; and</li> <li>• tell device resellers about the process; and</li> <li>• send devices of the replacement model to device resellers and merchants.</li> </ul>