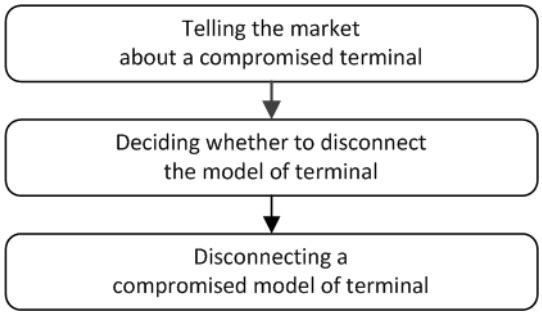
Appendix 13D: Compromised terminal disconnection plan

Purpose

This plan describes a 3-stage process specified in Part 8B of the Payments NZ (PNZ) rules for disconnecting a model of terminal from the EFTPOS switching network if:

- the terminal 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 terminal.

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 terminal quickly and efficiently,
- include stakeholders who are not PNZ participants in the process,
- ensure effective oversight of the process,
- 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 PNZ rules and standards bind participants and PNZ 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 PNZ and participants.

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

People involved in the process

The following table describes those affected by the 3 stage process:

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

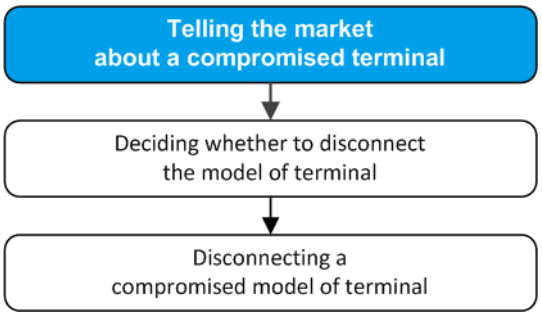
Contents

The plan describes the process in the following sections:

Section A: Communicating a compromise

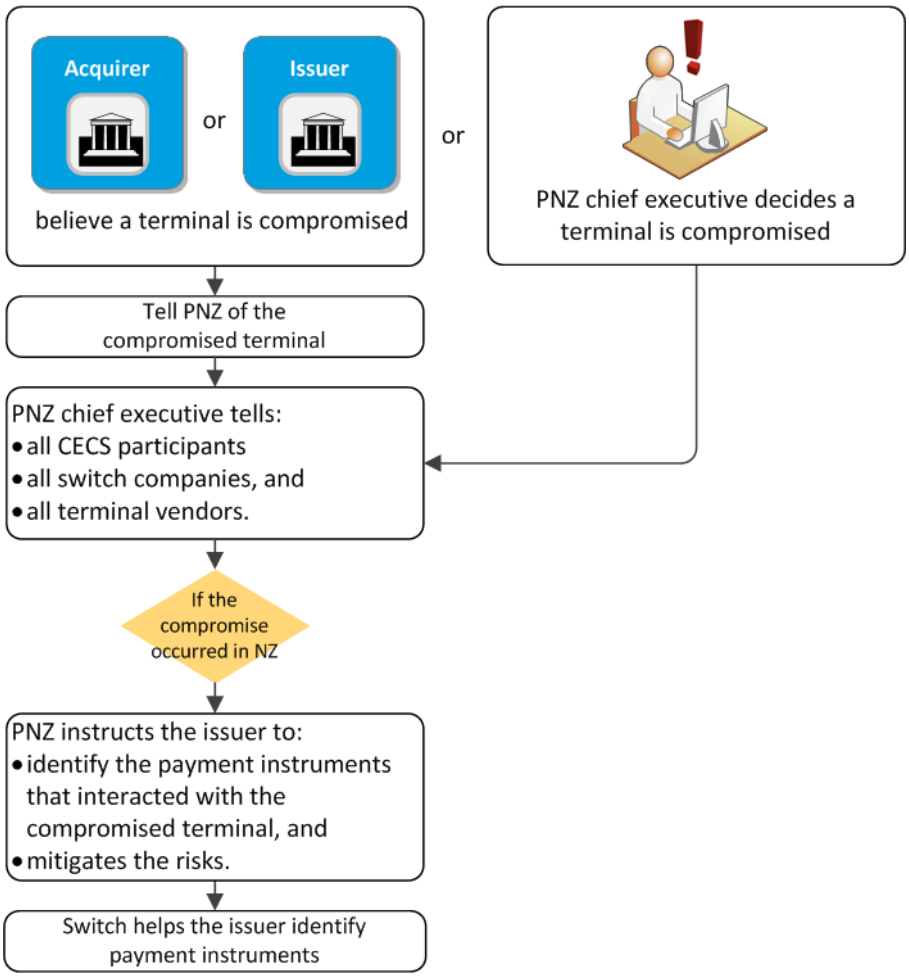
1st stage

During the 1st stage in the PNZ compromised terminal disconnection process, acquirers, issuers, PNZ, switches and terminal vendors communicate with each other about the failure of a terminal 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

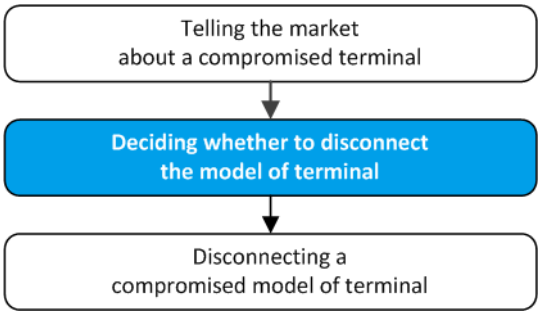
The following table summarises the roles and responsibilities of those involved in the 1st stage of the process:

Person	Description
Acquirer	• If acquirer believes a terminal has failed to protect sensitive data on a card or a payment application on a mobile device, notify PNZ. • Require its switch to help issuers identify payment instruments that have interacted with the compromised terminal.
Issuer	• If an issuer believes a terminal has failed to protect sensitive data on a card or a payment application on a mobile device, notify PNZ. • Identify every card or payment application on a mobile device issued by the issuer that has interacted with the terminal. • 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 card holder of the interaction with the terminal or cancelling the card).
PNZ	• Receives notifications of a terminal's failure to protect sensitive data or decides a terminal has failed to protect sensitive data for any other reason. • Notifies participants, switches and terminal vendors of the failure to protect sensitive data on a card or a payment application on a mobile device. • Instructs issuers to: – identify each payment instrument issued that has interacted with the terminal, and – 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 card holder of the interaction with the terminal or cancelling the card). • Instructs the acquirer who acquires transactions from the terminal to require its switch to help issuers identify cards or payment applications on mobile devices that have interacted with the terminal. • Communicates with media about the terminal compromise
Switch	• If requested by an issuer, help the issuer to identify payment instruments issued by the issuer that have interacted with the terminal.

Section B: Decision to disconnect

2nd stage

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



For a terminal compromise in New Zealand, during the 2nd stage in the process,:

- acquirers, switches, issuers and the terminal vendor have 48 hours to recommend to PNZ whether to disconnect the compromised model of terminal from the EFTPOS switching network, and
- PNZ (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 terminal compromise overseas, during the 2nd stage in the process, the CECS management committee and the board determine whether to disconnect the model of terminal at the next scheduled meetings of the committee and the board.

Contents

This section describes the following topics:

B1: NZ compromise: affected parties recommend

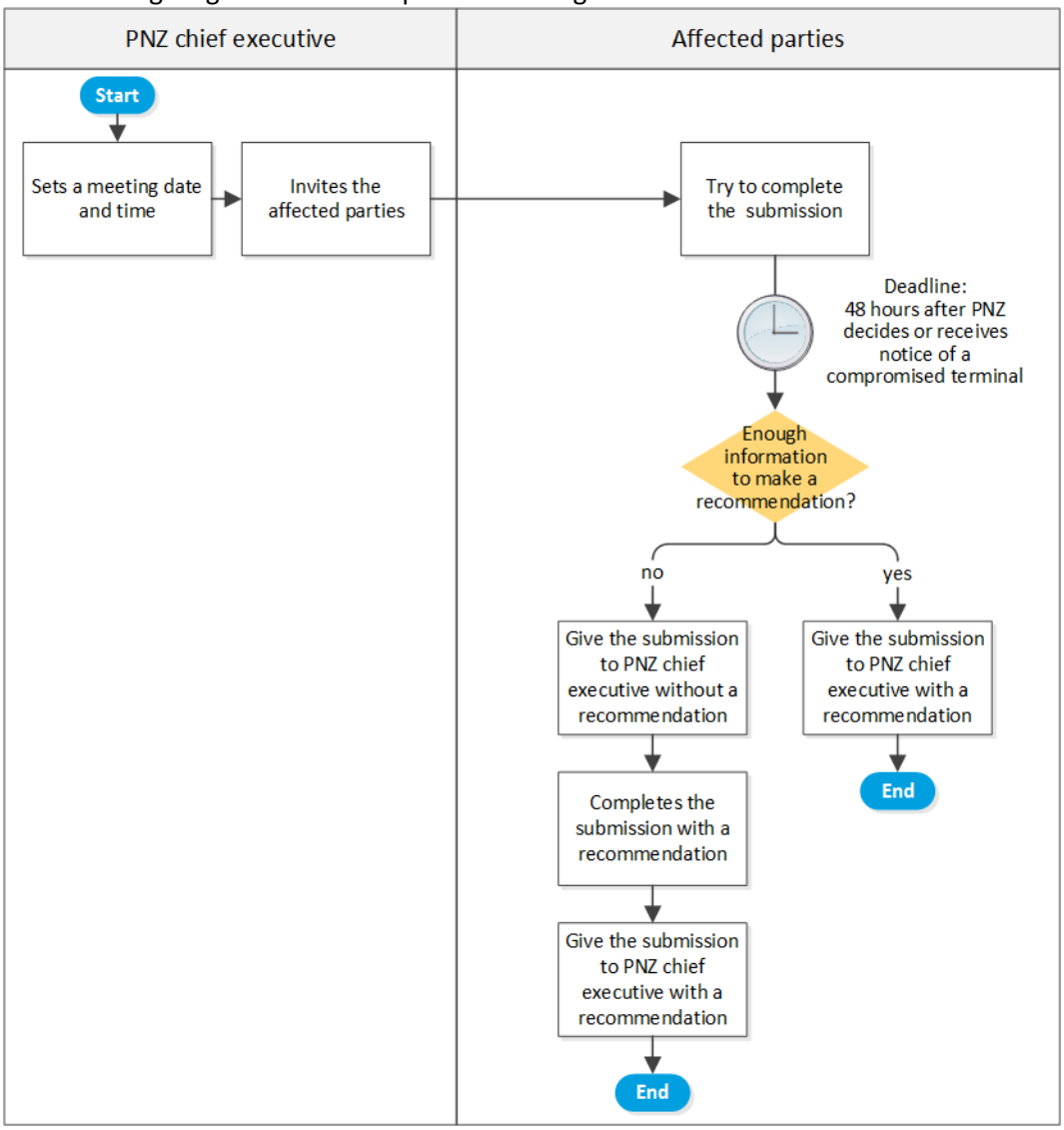
Process overview

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

- review the causes and consequences of the terminal's failure to protect sensitive data on a payment instrument, and
- recommend to PNZ whether to disconnect the model of terminal from the switching network.

The affected parties put the information and the recommendation in a submission for the PNZ CECS management committee and the PNZ 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:



PNZ arranges meeting to complete submission

To arrange a meeting of affected parties, the PNZ chief executive:

#	Action
1	• **invites** the those specified on the compromised terminal contact list for: – the terminal vendor who applied for registration of the model of terminal on the PNZ terminal register, – every switch company that connects terminals of the model to the EFTPOS switching network, – every acquirer who connects terminals of the model to the EFTPOS switching network, – every issuer who issued a payment instrument that interacted with the compromised terminal, and • for each representative invited, **uses** the email address specified on the compromised terminal contact list.
2	• may use the notice specified in terminal form 3 to invite the affected parties to the meeting, and • may attach the following to the notice: – the agenda specified in compromise terminal form 4, and – the submission template specified in appendix 13 C.

Affected parties' meeting

At the meeting of affected parties:

#	Action	
1	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 terminal to prevent: • an adverse effect on the integrity or the reputation of CECS, or • introduction of significant risk into CECS. The affected parties decide within 48 hours of the PNZ chief executive receiving notice of the compromise or deciding that a compromise has occurred.	
2	**If the affected parties decide…**	**then…**
	the affected parties can make a recommendation within the 48 hour deadline,	• the affected parties **complete** the submission and include the recommendation, and • the PNZ chief executive arranges meetings of the CECS management committee and the board and sends them the submission.
	the affected parties do not have enough information to make a recommendation within the 48 hour deadline,	• the affected parties complete as much of the submission as practicable **without including a recommendation**, • the PNZ chief executive – sends the incomplete submission to the CECS management committee and the board, – requires the affected parties to make a recommendation as soon as practicable, and – arranges meetings of the management committee and the board when the affected parties make a recommendation.

Roles and responsibilities

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

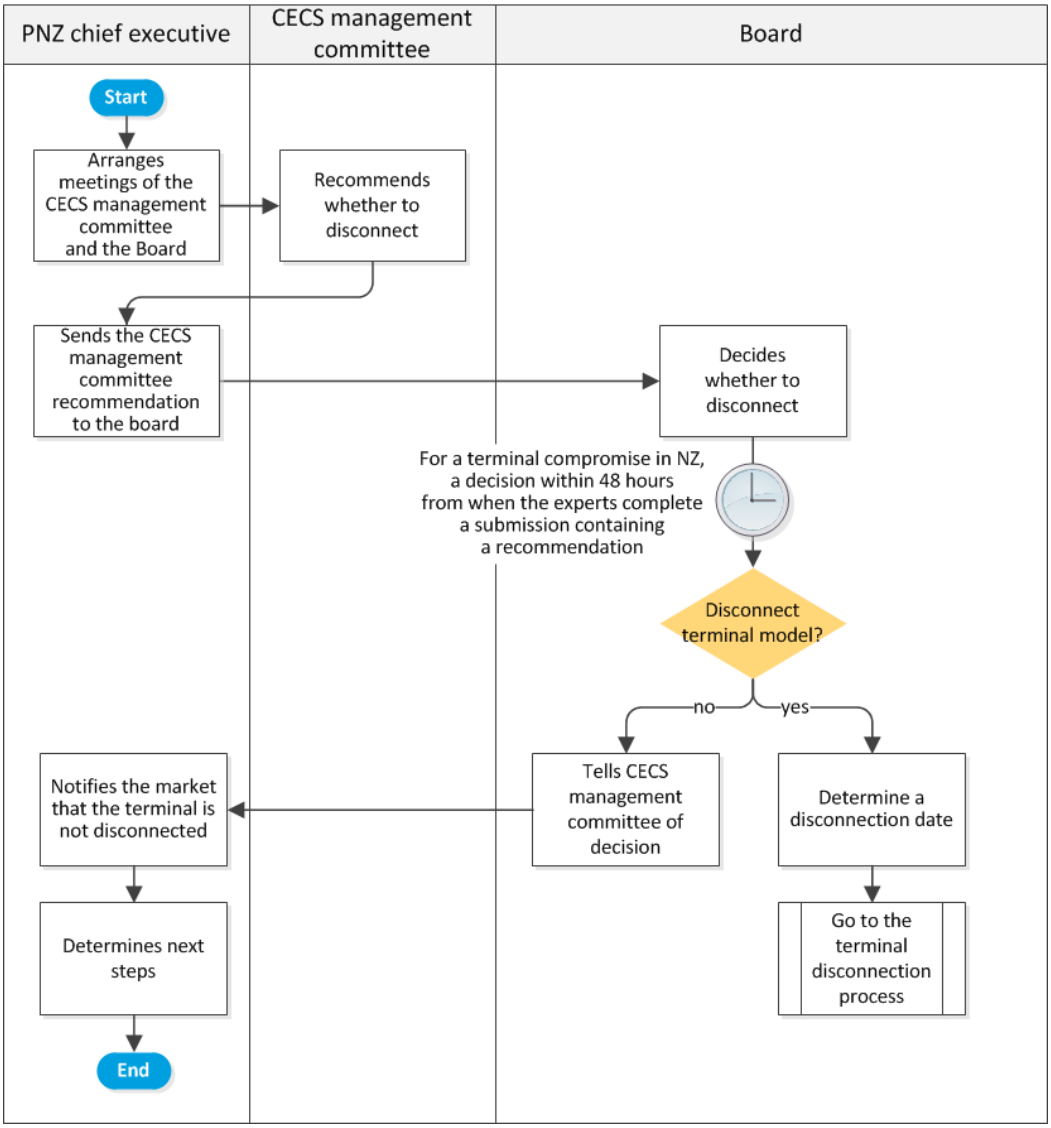
Person	Roles and responsibilities
Acquirer	If an acquirer is invited to the meeting of affected parties: • attend the meeting, • try to provide the information that PNZ requires for the terminal compromise submission as soon as practicable after PNZ requests the information, • arrange any reports required by PNZ in respect of the terminal compromised or the merchant operating the terminal, for example, a forensic report or a police report, • provide PNZ with the details that PNZ requires of the reports, • during the period in which the affected parties complete the terminal compromise submission, monitor the market to determine whether any other terminal connected to the EFTPOS switching network fails to protect sensitive data on a payment instrument, and • help PNZ to coordinate and lead meetings of the affected parties.
Issuer	If an issuer is invited to the meeting of affected parties: • attend the meeting, and • try to provide any information that PNZ requires for the terminal compromise submission as soon as practicable after PNZ requests the information from the issuer.
PNZ chief executive	• arranges the meeting of affected parties, • leads and attends the meetings, • records the decisions of the affected parties in the terminal compromise submission, • updates the CECS management committee and the Payments NZ board on: – the affected parties' progress towards completing the submission, and – when the committee and the board may be required to decide whether to disconnect the model of terminal, and • communicates with media about the terminal compromise
Switch	If a switch is invited to the meeting of affected parties: • attend the meeting, and • try to provide any information that PNZ requires for the terminal compromise submission as soon as practicable after PNZ requests the information from the switch.
Terminal vendor	If a terminal vendor is invited to the meeting of affected parties: • attend the meeting, and • try to provide any information that PNZ requires for the terminal compromise submission as soon as practicable after PNZ requests the information from the terminal vendor.

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 terminal from the EFTPOS switching network, and
- the board decides whether or not to disconnect the compromised model of terminal from the EFTPOS switching network and, if it requires disconnection, a disconnection date and a date from which terminals of the model cannot connect for the first time to the EFTPOS switching network.



Roles and responsibilities

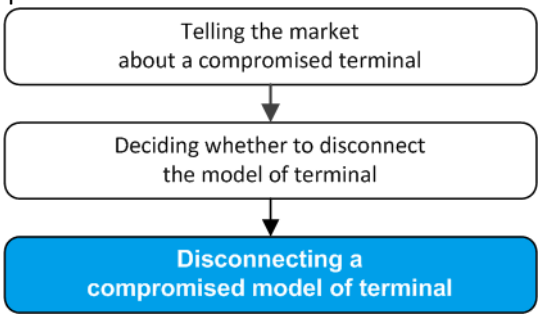
The following table summarises the roles and responsibilities of those involved in the decisions of the CECS management committee and the board:

Person	Roles and responsibilities
Acquirer	Make submissions to the committee or to the board
Issuer	Make submissions to the committee or to the board
PNZ	Communicates with media about the terminal compromise
Switch	Make submissions to the committee or to the board
Terminal vendor	Make submissions to the committee or to the board

Section C: Disconnection process

3rd stage

The highlighted block in the following diagram shows the 3rd stage in the compromised terminal disconnection process described in this section:

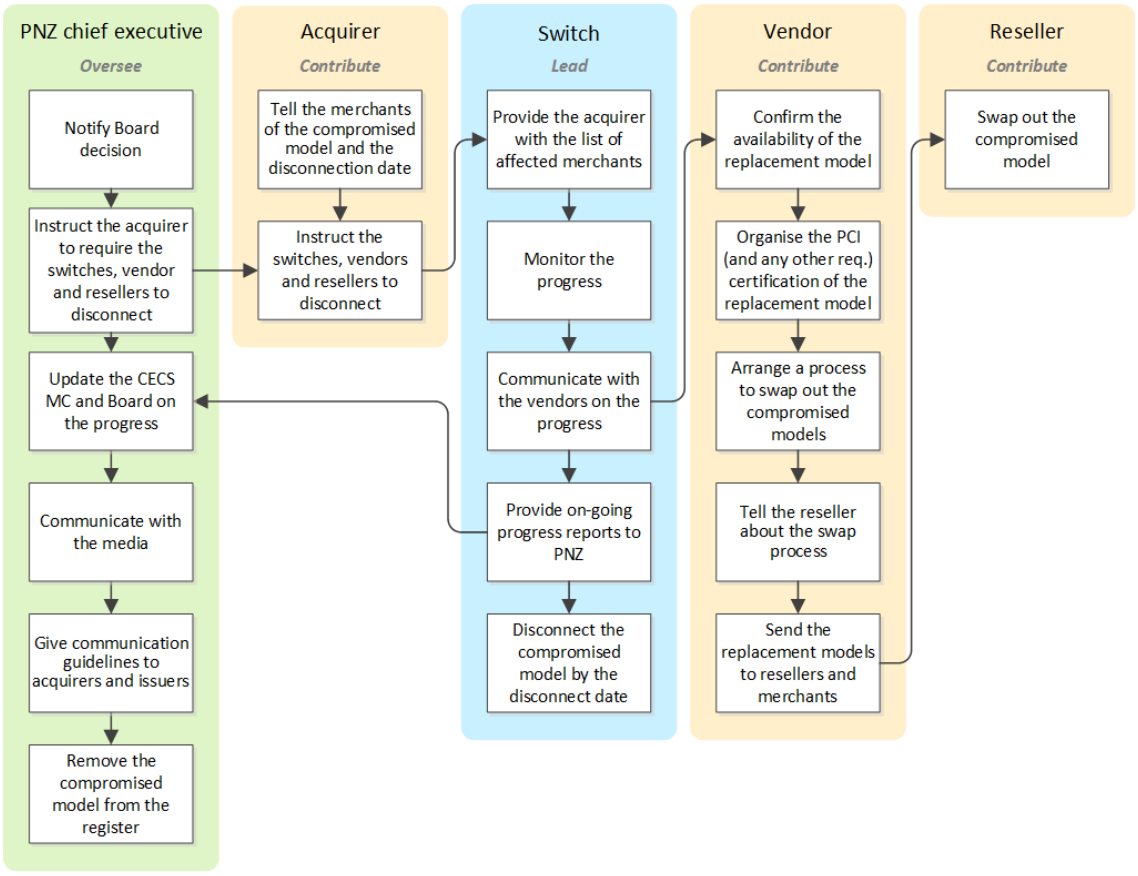


If the PNZ board requires disconnection of a compromised model of terminal from the switching network, during the 3rd stage in the process the following work together to disconnect it and replace it with a different model:

- acquirers,
- PNZ,
- switches,
- terminal resellers, and
- the terminal 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
Acquirer	• tell merchants who operate the compromised model of terminal of the board's decision to disconnect the model of terminal, the disconnection date and that the merchant will require a replacement terminal of a different model no later than the disconnection date • comply with PNZ's instructions by requiring switches, the terminal vendor and terminal resellers to take the steps specified by the PNZ rules to disconnect and replace the compromised model of terminal.
PNZ	• using compromised terminal form 2,: – notifies participants, switches and terminal vendors of the board's decision and the disconnection date, and – instructs acquirers to require switches, the terminal vendor and terminal resellers to take the steps specified by the PNZ rules to disconnect and replace the compromised model of terminal, • communicates with media about the terminal compromise and the disconnection process, and • gives guidelines to: – acquirers for communicating with media and merchants about the compromise and the disconnection process, and – issuers for communicating with media and customers about the compromise and the disconnection process.
Switch company	Comply with acquirers' instructions to: • tell acquirers the names of merchants operating the compromised model of terminal, • manage and monitor the disconnection and replacement process, • manage communications with the terminal vendor about the disconnection and replacement process, • during the disconnection and replacement process, tell PNZ when PNZ requires of the number of terminals disconnected and replaced, • on the no new connections date, prevent terminals of the compromised from connecting for the first time to the EFTPOS switching network, and • by the disconnection date, disconnect the compromised model of terminal.
Terminal reseller	Comply with a terminal vendor's instructions to replace the compromised model of terminal with the replacement model of terminal.

Person	Role and responsibility
Terminal vendor	Comply with a switch company's instructions to: • determine the number of terminals of the compromised model to be disconnected and replaced with a different model of terminal, • confirm whether the vendor can replace every terminal of the compromised model with a different model of terminal by the disconnection date, • determine any functional differences between the compromised model of terminal and the replacement model of terminal and ensure that the replacement model of equal functionality at least, • if the replacement model of terminal is not registered on the PNZ terminal register, apply to PNZ to register the model of terminal, • if the replacement model of terminal requires approval from any other entity (e.g. a switch) before connection to the EFTPOS switching network, arrange to get the approval, • arrange a process to disconnect terminals of the compromised model and replace them with terminals of the replacement model, • tell terminal resellers about the process, and • send terminals of the replacement model to terminal resellers and merchants.