FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

APRIL 2024

Notification of incidents relating to the operational resilience of technology systems

Some regulated entities are required to notify the Financial Markets Authority – Te Mana Tātai Hokohoko (FMA) of any event that materially impacts the operational resilience of their critical technology systems (material incident). This includes an event that materially disrupts or affects the provision of the entity's market service or has a material adverse impact on recipients of that service (e.g. consumers or investors).

To confirm if these requirements apply to you, refer to your market services licensee conditions. Information about your obligations can also be found on the FMA website.

Business continuity and technology systems online form

We have an online form for notifying material incidents. Regulated entities that are required to notify incidents to us can use the form to securely provide key information about the incident.

The following pages set out the questions you will be asked when notifying us of an incident. This is for information only; all notifications must be made via the online form, which can be accessed through the FMA Online Services portal.

The form is dynamic. You will only see questions relevant to the options you select. For example, if you do not indicate the incident has been resolved, you will not see the questions requesting this information.

If some details are not available at the time you are notifying us of the incident, you will need to provide these to us as soon as possible, and provide updates until the incident has been resolved. The form is designed to be used for initial reporting, providing updates on developments, and submitting a concluding report once the reported incident has been resolved. We may also request additional information about the incident.

For entities that must report material incidents to the Reserve Bank of New Zealand and the FMA, you will have the option to either complete the questions in the form, or upload the Material Cyber Incident Notification Report Template required by the Reserve Bank.

If you are unable to access Online Services, you can call 0800 434 566 or email compliance@fma.govt.nz.

What you will be asked

Notifications – Identification

What would you like to notify us about?

Please enter the Financial Service Providers Registry number of your Notifying Entity.

Are the entity details shown above correct and do you have authorisation to notify on their behalf?

- Yes
- No

How would you like to proceed?

- Complete the FMA's online notification form
- Upload RBNZ's Cyber Material Incident form

If select "Complete the FMA's online notification form" the filer will be directed to the online notification questions.

If select "Upload RBNZ's Cyber Material Incident form", the filer will be directed to the upload page to upload the completed RBNZ template. The filer will not be required to answer any questions in the form and will be directed to the Declaration page after uploading the RBNZ template.

Before You Begin

Instructions for this Business Continuity and Technology Systems incident notification.

Business Continuity and Technology Systems incident notification

From the options available below, select one that most applies to this incident reporting.

- Initial notification of incident, not resolved
- Initial notification of incident, already resolved
- Update on existing notification, not resolved
- Update on existing notification, resolved

Enter the unique incident ID assigned by your organisation.

Event details

Do you know the date that this incident occurred?

- Yes
- No

If selected “yes”, please enter the date and time that the incident occurred.
Enter the date and time that your business became aware that the incident had occurred.
What is the current state of the incident? • Active • Under investigation • Mitigated • Resolved
Classify the severity of this incident. • Severe • High • Moderate • Low
Type of incident
Which type of incident are you reporting on? • Cyber attack • Internal outage/Service Failure
If select “Cyber attack, please choose which type of cyber attack you experienced. • Phishing or Credential Harvesting • Scams & Fraud • Unauthorised Access • Malware Infection against the entities system • Website Compromise • Network Attack • Ransom Demand received • Distributed Denial of Service attacks • Other
If select “Internal outage/Service failure, please choose which type of outage or service failure you experienced. • Network Failure • Infrastructure Failure • Capacity Management issue • Core Banking outage • Data compromised or lost • Application Outage • Supplier Failure • Other

How was this incident detected? • Internal controls • Outage notification • Cyber attack detection notification • Cyber security vulnerability alert • Outsourced provider notification • Frontline staff/partners notification • Digital channel availability (e.g. website) • Customer notification • Staff compliance breach notification • Other
Which of these are impacts of this incident? • Customer impact • Transactional failure • Processing unavailability • Unknown
If select “Customer impact”, please choose which types of customer channels are affected by this incident? • ATM • Branch/Store network • Contact centre • Digital services (mobile) • Digital Services (Web) • Data Loss • Unauthorised disclosure of personal information • Financial loss to customers • Unable to access core services • Other
If select “Transaction failure”, please choose which type of transaction failure was affected by this incident? • Customer payment failure • Domestic interbank payment failure • International payment failure • Deposit processing failure • Lending processing failure • Credit card processing failure • Other

If select “processing unavailability”, please choose which types of processing were unavailable due to this incident?

- Operations processing
- Application processing
- Claims management
- Other

Have any of these categories of customer, been impacted by this incident?

- Government
- Corporate
- Business
- Retail
- Other
- None

Do you know the number of customers impacted by this incident?

- Yes
- No

If select “Yes”, enter your estimate of the number of customers affected by this incident.

If possible, please estimate the percentage of your total customer base, impacted by this incident.

- <10%
- =>10% to 25%
- =>26% to 50%
- =>51% to 75%
- =>76% to 100%
- Unknown

Have any of these customer products been impacted by this incident?

- Credit/lending
- Deposit taking
- Payments
- Investments
- Insurance
- Financial advice
- Financial markets (Treasury)
- Fund Management
- Crowd Funding
- Other customer products
- None

Impacts of this incident
Has your business continuity plan activated for this incident? • Yes • No
Has a viable solution been identified? • Yes • No
If select “Yes”, please summarise this viable solution.
Do you have an estimate of how long it will be until all interruptions to services will have concluded? • Yes • No • All interruptions to services have concluded
If select “Yes”, enter when you expect all interruptions to services will have concluded?
Is the root cause of this incident known? • Yes • No
If select “Yes”, please describe the root cause identified.
Has this incident attracted media attention? • Yes • No
Has this incident caused regulatory impact, or do you anticipate it may? • Yes • No • Unknown
If select “Yes”, please describe the regulatory impact and please describe any actions taken, to prevent further impacts from this incident.

Who else has been notified of this incident? • RBNZ • NCSC • CERT NZ • APRA • ASIC • OPC • Trustees (for NBDTs) • Other • None
Incident resolved
Enter the date that this incident was resolved.
Has there been a post incident report prepared? • Yes • No
If select “Yes”, was this post incident review an independent report? • Yes • No
Enter what additional steps have you taken, or about to take, to address this problem in the longer term.
Provide a summary of your implemented solution.
List the corrective actions taken to prevent future occurrences of similar types of incident.
Declaration
I confirm that I have the authority to submit this report on behalf of [the reporting entity name].
I have reviewed the answers and information and I confirm that I am satisfied that, to the best of my knowledge, after undertaking all reasonable inquiries, all answers are true and correct.
Full name of the authorised person.
Position/Job title of the authorised person.
Date: [This will pre-populate the current date] Mobile number: [This will pre-populate the mobile number of the authorised person] Email: [This will pre-populate the email address of the authorised person]