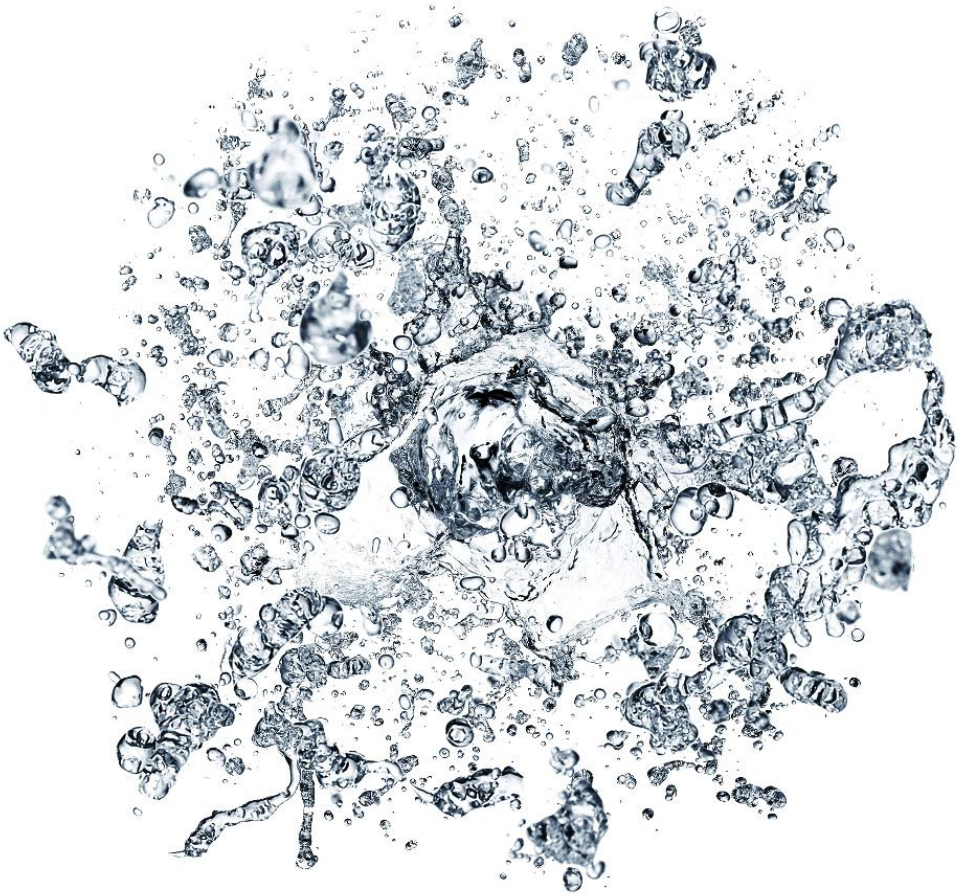
Deloitte.



Reserve Bank of New Zealand

Information Breaches

February 2021

Executive Summary

Background to the investigation

1. The Reserve Bank of New Zealand (RBNZ, the Bank) informed us that it had experienced two information breaches, one of which occurred internally, and one where market sensitive information was released externally, prior to when this information was intended to be in the public domain. We were advised that the two specific incidents occurred on:

    a. 6 November 2020 –Sensitive information contained within a draft RBNZ Chief Executive (CE) Report to the Board (Internal Breach).

    b. 11 November 2020 – Letter sent by RBNZ to Non-Bank Deposit Takers (NBDTs), prior to the 2pm Monetary Policy Statement Announcement (MPS) (External Breach), in relation to the Funding for Lending Programme (FLP).

2. As a result of these breaches, RBNZ engaged Deloitte to undertake an independent investigation to help RBNZ better understand what occurred and to understand what improvements can be made to the Bank's handling of sensitive information.

Scope of the investigation

3. This report is a summary report of the investigation for public release. The scope of the investigation that is reported on in further detail in the full report[1] was to:

    a. Understand the timeline of events and the scale of the breaches.

    b. Conduct an examination of the process gaps or control failings that led to the breaches. This is to include awareness of previous audit findings/recommendations to understand if there are thematic or systemic issues.

    c. Undertake an analysis of whether the Post Incident Response and actions taken to mitigate/remediate the breaches were sufficient and appropriate.

    d. Make recommendations on what improvements can be made to the Bank's handling of sensitive information and incident response processes to ensure this does not recur.

Our findings

<u>Incident One – Draft Chief Executive Report</u>

4. Based on the scope of our work, we have established that during the preparation of the November 2020 CE Report, information was inadequately identified and 'marked' as market sensitive when it was included in the draft report. This information was initially incorrectly sent to the staff member collating the CE Report on 3 November 2020 (the first breach), and was then uploaded to a location which was accessible to all Bank employees on 4 November 2020 (the second breach).

5. There are several factors which, in our view, contributed to the two breaches occurring. These are:

    a. Some of the individuals involved in collation and preparation of the draft report were relatively new employees and were not familiar with what comprises market sensitive information in RBNZ's context. These employees had not received training on what constitutes market sensitive information.

    b. The CE Report template that contained the information was not marked at any time to reflect that this contained market sensitive information. Identifying and appropriately classifying market sensitive information is not ingrained in the culture at RBNZ.

    c. There was a change of process, which resulted in the request for the CE Report content (Call Up) and the Balanced Scorecard being combined, as opposed to separate Call Ups (which was the historic process). As part of combining the Call Up of the two reporting documents, the CE Report template had been moved from a locked

[1] Provided to RBNZ in January 2021

directory folder to a new location. The movement of this folder changed who would be able to access the information. It was not clear to those updating the CE Report that it had been moved.

d. When the new file location was established, no consideration was given as to who was able to access the new location, or whether user access rights should be considered and managed.

e. The Call Up request was not clear as to whether the templates were to be updated through a link, or sent via email to either of the two staff members referred to in the request.

Incident Two – NBDT Letter

6. We have established that an external release of market sensitive information did occur on 11 November 2020. A letter which contained market sensitive information in relation to the FLP was disclosed by email to 18 NBDTs during a six-minute period between 1:14 pm and 1:20 pm. This is approximately 45 minutes prior to the information being communicated by the Bank at 2:00pm, in a planned Monetary Policy Statement announcement. These letters were addressed to a member of each NBDT's Senior Leadership Team and were emailed to their specific email address. In addition to the 18 NBDTs that received this information, the letter was also released to an external lawyer representing several NBDTs, along with two RBNZ staff, who were copied into the correspondence.

7. Following the emails sent between 1:14pm and 1:20pm, the sender attempted to recall the email, however this was not successful. The letters were then resent to the initial recipients between 3:27 pm and 3:31 pm.

8. In addition to the external breach, there was an internal breach within the Bank, prior to the release of the information on 11 November 2020. The internal breach occurred on 9 November 2020, when the same individual who sent the NBDT letter saved a draft version of the document that was being prepared, into Documentum. Documentum is the document management system used by the Bank. At this point, the draft document became available to 233 Bank staff who had the user access rights to view this document. While the version tracking on the underlying document records indicate that only the sender "checked out" this document, we have been unable to ascertain whether any other Bank staff accessed the document.

9. There are several factors which, in our view, contributed to these breaches occurring. These are:

a. The letter to the NBDTs was designed to be a response to earlier correspondence with the sector and was not intended to be released prior to the 2pm MPS Announcement (i.e. it was not considered by the Bank that this letter would disclose the FLP to the NBDTs). As such, the processes and controls for the handling of market sensitive information in relation to the MPS Announcement, including the involvement of the Communications team, were not engaged.

b. There was an awareness between the team who prepared the letter that it contained market sensitive information, but it was not marked as market sensitive.

c. As the letter was a response to earlier correspondence, and included commentary on the FLP, it was prepared across several Bank teams. The process included staff in the Financial Stability Group (FSG) who would not normally be involved in an MPS communication. This meant that the letter was sent by an individual who was not familiar with the MPS process.

d. When the document was saved to Documentum, there was no consideration as to who was able to access the new location and document, or whether user access rights should be considered and managed.

e. There was no predetermined or documented incident response plan, which would have aided Bank staff with a more timely escalation to the Senior Leadership Team.

Policy, Process and Control Improvement Opportunities

10. There are few organisations in New Zealand that are responsible for the creation, management, and handling of market sensitive information as frequently as the RBNZ. This results in RBNZ, by the nature of its role, being susceptible to unique challenges and risks. This subsection outlines the opportunities we identified for the Bank to improve its policy, processes and controls.

People

11. The Bank utilises subject matter experts with specialised knowledge to provide information and input across the Bank. Despite the Bank's staff being highly skilled, new and long-term staff members may not fully understand the operational risks that the organisation has when creating, handling, and passing on market sensitive information. We found that it is not ingrained in the Bank's culture to be considering the identification and classification of market sensitive information.

a. Both incidents involved staff members who had not been in their current roles for a long period of time. This indicates that new RBNZ employees are not familiar with Bank processes and procedures, specifically related to identifying, classifying and treating market sensitive information.

b. In addition, senior members of various teams reviewed documents that contained market sensitive information but did not identify the need to treat and mark the documents as such, including limiting the number of people that had access to the information. This indicates that the responsibility of identifying and marking sensitive information is not clear.

c. RBNZ employees advised that there is no internal education leading to improved awareness levels regarding the management of sensitive and confidential information. It was indicated that employees are expected to learn from their current team leads; however, there is no formalised training or ongoing education on this topic.

Policies and processes

12. RBNZ has advised us that there are currently 96 policies across the organisation. The Bank is currently undertaking an initiative for these to be reviewed and streamlined. In the table below, we provide our view of the following policies that were provided to us:

Policy	Relevant Policy Information	Our assessment of the policy and associated procedures
Acceptable Use Standard	• Transmission of sensitive information: Sensitive or confidential information must not be sent via email to any address outside the Bank without secure encryption. • Information management: Bank documents must be assigned security classifications depending on the sensitivity of the information. This applies to both physical and electronic documents. All bank information and data must be stored in approved information repositories.	The following are not documented: • The expectation of using links and/or attachments in emails. There is no guidance on requirements for password protection of documents that are emailed. • No set standard for the classification of email / correspondence. • The responsibilities of classifying the documents (preparer versus reviewer). • Information is sensitive right up until the time that it is released to the market and needs to be treated as such (even if intended to be non-disclosive).
Access Management Standard	• Periodic access reviews: All user accounts are reviewed annually by the Information Security manager and the respective business owners. This ensures that users have access only to the functionalities that they need in their current roles and also serves as a	RBNZ has advised that the following do not occur: • Documented annual user access reviews. • Review of the access logs on a regular basis.

Policy	Relevant Policy Information	Our assessment of the policy and associated procedures
	check for the user de-registration process. • Monitoring and alerting: RBNZ Information Security Manager reviews all access logs on a regular basis. • User awareness and expectations: Formal procedures or standards shall be developed for handling and storage of information assets based on their classification, to protect the information assets from unauthorised disclosure or misuse.	In addition, there are no formalised procedures within the Bank regarding handling or storage of information based on its classification.
Records Management Policy	• Managers are responsible for: o Ensuring all team members are aware of this and related policies. o Ensuring all new staff receive Documentum training. o Ensuring the appropriate security measures are observed for maintaining records containing personal or other restricted information. • Monitoring and Review: The following activities are undertaken to ensure compliance with this policy. o Quality assurance of the file plan, deleted items via daily reports. o Internal audits. o External audits as part of the Public Records Act Audit Programme.	• There is no current documentation of the expected usage of Documentum. In addition, training for Documentum is the responsibility of each manager, which may lead to inconsistencies in understanding its purpose and using the document repository. • There is no documented process for adding new folders and considering where documents are saved on Documentum. • There have been no quality assurance reviews, or internal or external audits conducted relating to records management.
Information Access, Security and Classification	• The following classification categories are specified: o In-confidence o Sensitive o Restricted o Confidential o Secret o Top secret.	• These classification categories are not available for selection during document creation, which means that even though classification categories are defined, they cannot practically be applied by RBNZ users. • The policy does not specifically provide guidance relating to the handling and sharing (internally and externally) of information in 'market sensitive' categories. There is no procedure which outlines the steps required for managing sensitive or market sensitive information throughout its lifecycle.

13. Profiles for new employees are generally replicated from the profiles of users in a similar role for new user access system set up. This has resulted in privileges not being commensurate with a user's job functions.

14. RBNZ does not perform any formal reviews or attestation of user access rights to confirm that the level of access provided remains appropriate and relevant to the role they are performing within the organisation, which results in users having more privileges than are required to perform the activities related to their role. The security team is in the process of implementing role-based access control and have wider identity governance and management activities planned for FY2022.

Technology

15. Currently, the Bank utilises Documentum but there is a lack of understanding of the usage of the document repository and the potential risks and implications. There is the potential to consider whether email is the most suitable means for correspondence of sensitive information and whether a better system can be put in place for the release of information (e.g. secure file transfer site). If email is required, clear guidance and requirements regarding password protecting/encrypting documents should be established.

16. RBNZ does not currently have any mechanism for detecting sensitive information leaving the Bank or facilitating the approval and release of sensitive information. All potential detective controls for data protection, such as Data Loss Prevention (DLP) or Cloud Access Security Broker (CASB), would require documents to be classified to allow alerts to trigger in the event of a potential data breach, as the rule sets for these solutions would be created around the defined classification categories. This means that even if RBNZ had implemented technology controls to mitigate the release, upload or local storing of sensitive information, this would not be effective without information being classified in accordance with its sensitivity.

17. There is no process or control which approves the release of the emails containing documents which contain market sensitive information, which means that the release at the target time will always be dependent on a single individual within the Bank. There is also no solution in the current technology portfolio which can support a system-driven automatic release at the target time.

    The current technology system would not have detected:

    a. New folders created with market sensitive documents.

    b. The early release of the NBDT letter.

Incident 1 – CE Board Report

18. There is no standard procedure which stipulates that documents that are likely to contain sensitive information (such as the CE Report) should always be treated as a document with a sensitive classification from creation through to release. Again, this would be dependent on the ability to easily classify information within the Bank and having clear procedures for the handling of each classification category.

19. Due to the staff members responsible for collating the documents being new to the Bank, there was a lack of understanding that the information being gathered was considered market sensitive. There is a need for establishing and communicating (regularly):

    a. What should be classified as market sensitive information;

    b. The implications of access to market sensitive information not being appropriately restricted;

    c. How to decide on access and to apply restriction levels (e.g. locked folders); and

    d. The responsibilities of treating and marking the documents that are market sensitive.

20. Regarding Documentum, there is no documented policy outlining expectations of using the system, adding new folders (and locking folders) and considering where documents are saved. The policy should clearly state the expectations that all documents remain in Documentum and not be saved or updated on Bank staff's local drives. This will retain the most

up to date version without creating multiple versions across individual's local drives. This will also limit access to any market sensitive information as they remain in locked Documentum folders.

Incident 2 – NBDT Letter

21. The NDBT response letter was intended to be a non-disclosive response; however, it included the FLP decision which results in the whole document being classified as market sensitive.

22. It is both the responsibility of the writer of the letter and the reviewer to identify that market sensitivity and to ensure the information is restricted and released at the correct time.

23. In this instance, the individuals did not mark that the letter was market sensitive and the assumed MPC decision was pre-populated into the letter. The documents can be prepared prior to the MPC decision; however, any specific assumptions or details relating to MPC decisions should not be populated until after the decision has been made.

24. The Bank has advised us that if the sender of the documents had not raised the issue of the release of information prior to the intended time, it would not have been identified by any existing controls at the Bank.

25. A review of the Economic team and the MPS end-to-end process was conducted by internal audit earlier in 2020. The two main recommendations were:

    a. Assessing user access to folders across Documentum and Diligent (platform to share information with Board members); and

    b. Accountability for any printed versions of market sensitive information (e.g. MPC papers).

    These align with the current issues/next steps to be rectified to prevent any future release of information before the intended time.

Incident Response Process

26. Incident Two was determined to be a critical incident. Under the PPI guidelines, the incident was of a nature that was required to be immediately escalated within 24 hours, which was met. However, the policy should be updated to have the incident escalated as soon as possible/practical. As there are no specific documented guidelines regarding handling the incident, this resulted in a delay in the immediate escalation of the breach which ultimately exposed senior RBNZ staff, as they were unaware of the issue whilst communicating with external stakeholders, including media.

27. Regarding Incident Two, once escalation of the breach had occurred, the Bank was reliant on the experience of senior team members to determine the steps to take.

28. There is no documented playbook or incident response guidelines to reference within the Bank. The incident response guideline should be established and communicated. The playbook should:

    a. Specify who should be informed;

    b. Identify key steps to be taken to minimise the impact of the breach;

    c. Establish actions that should be taken in relation to the investigation;

    d. Include clear protocols to determine the extent of the breach, assessing the impact, and informing key stakeholders;

    e. Incorporate a communications plan, which includes identifying key internal and external stakeholders, taking immediate communications related steps and prioritising any next steps;

    f. Utilise a rapid impact scenario assessment which would establish potential scenarios as a result of the breach and key next steps, timeframes, and owners.

Recommendations to improve RBNZ's handling of sensitive information

29. To improve the handling of sensitive information and reduce the likelihood of information breaches in future, RBNZ should:

a. Update the RBNZ Access, Security and Classifications Policy to specifically make provision for classification categories that the Bank would have, as opposed to using the generic Protective Security Requirements (PSR) classification categories, to make it easy for users to accurately classify information.

b. Create information handling procedures for each classification category defined in the updated policy, which stipulates where information may be stored, who it may be shared with and how it should be handled throughout its lifecycle.

c. Implement a solution which would enable the easy classification of files when created or received by Bank employees. This could be a new technology solution or enabling a feature of a solution that RBNZ has already implemented.

d. Run user awareness campaigns and training once the foundational components above have been developed and implemented, to drive the rapid adoption of the new procedures related to sensitive information.

e. Undertake a tactical review of the members of Active Directory groups providing access to Documentum folders which would likely contain sensitive information, to confirm that their role within the organisation would require access to the folder. Once this tactical review is completed, a wider review of all privileges for all employees should be undertaken.

f. Perform a review of user access within the Bank, to confirm that the access provisioned for each user is commensurate with their role within the Bank. These reviews should include sign off by management of each department to confirm that appropriate levels of access are provided.

g. Expedite the initiatives related to identity governance and management which the Bank has planned for FY2022, to enable the principle of least privilege to be applied and access to be controlled and managed centrally.

h. Treat all incidents related to sensitive information as a data breach, to make sure the relevant stakeholders are informed and the right process for response, communication and investigation are executed in a timely manner.

i. Create a playbook specifically for the management of incidents that relate to information breaches, with the key activities to undertake during the response process.

Limitations

30. We note the following limitations in respect of this report:

a. This report was prepared for the specific purpose of assisting the Reserve Bank of New Zealand;

b. No party may rely on this report or our work, without our express prior written approval. Deloitte accepts no liability whatsoever to any party who relies on our report and/or our work except to the extent set out in our engagement letter and Master Terms of Business;

c. We are not qualified to provide legal advice. Legal advice should be sought on legal matters;

d. This report has been prepared based on work completed as at 18 December 2020. We assume no responsibility for updating this report for events and circumstances occurring after that date;

e. We reserve the right, but are under no obligation, to alter the findings reached in this report should information that is relevant to our findings subsequently be identified;

f. For the purposes of preparing this report, reliance has been placed upon the material, representations, information and instructions provided to us. Original documentation has not been seen (unless otherwise stated) and no audit or examination of the validity of the documentation, representations, information and instructions provided has been undertaken, except where it is expressly stated to have been;

g. Information obtained by Deloitte includes information provided at interviews which may not be factually correct or capable of corroboration. As a result, no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by Reserve Bank personnel. We accept no responsibility for the reliability of the information provided to us to the extent it is inaccurate, incomplete or misleading, or for matters not covered by our report or omitted due to the limited nature of our work;

h. Our work does not constitute an assurance engagement in accordance with New Zealand standards for assurance engagements, nor does it represent any form of audit under New Zealand standards on auditing (International Standards on Auditing (New Zealand)). Consequently, no assurance conclusion nor audit opinion is provided. We do not warrant that our enquiries will identify or reveal any matter which an assurance engagement or audit might disclose;

i. Deloitte is not responsible for ensuring any party's compliance with the requirements of the Privacy Act or similar requirements in other jurisdictions.

Deloitte.