INCIDENT REPORT

PROVISION OF HIGH RESOLUTION BANKNOTE IMAGES TO

The Incident

a website developer, has been retained by the Bank to develop a banknotes-related micro-site.

On 23 June 2011, as part of the development work underway, a DVD containing a variety of images, including images of banknotes, was sent by courier to for use by its designers. This DVD contained banknote images of a resolution quality greater than 72 dpi. The Bank's reproduction guidelines state that banknote images greater than 72 dpi should not used by outside parties. There were 249 images on the DVD, of which 160 were high resolution partial or full images of banknotes.[1]

This incident resulted from a misunderstanding by the staff member involved regarding the application in this case of Note Issue's reproductions guidelines and an error of judgement relating to the action that was taken. The incident also highlights that more stringent checking of images that leave the department may be needed.

Remedial Action

Upon realising the error that had been made, Account Director was immediately contacted to inform him that certain images on the DVD should not have been sent to the company and to request that any images placed onto company servers and computer drives be deleted. Digital Producer subsequently advised that no copies of any images had been made, and that the DVD had not been used in any way.

The incident was also immediately drawn to the attention of the Senior Manager, Communication and the Head of Note Issue.

The following morning a Note Issue staff member retrieved the DVD from where it had been stored in a locked drawer. It was still in its unopened courier packaging, indicating that the DVD had not been used.

All External Relations team members have been reminded of the reproductions guidelines and that no high resolution images of banknotes are to be provided to outside parties without prior consultation with senior management.

Risk Assessment

In the period between 23 June and 5 July, there was a risk that high resolution banknote images could have been copied, stored and potentially misused by staff members or by other outside parties via contacts with This could have had reputational consequences for the Bank.

Remedial action taken together with the confidentiality arrangements in place with has satisfactorily mitigated this risk.

A review of Note Issue's risk registers indicated that the risk of contravention by Note Issue of its own reproduction guidelines without the prior approval of senior management is not covered. A new risk entry will be created in the NI - General Operations Risk Register.

---

[1] For the purpose of this note, 'low quality' images are defined as those of 72 dpi or less, and 'high quality' images are defined as those with dpi great than 72.

Action Plan

To further mitigate the risk of inadvertently supplying high resolution images to other parties, the following actions have been identified:

- Counsel staff involved in the need to ensure that senior management is consulted prior to taking any actions that would be outside established policy or guidelines (completed).
- Establish arrangements to remind External Relations staff periodically through the annual risk review process of the reproduction guidelines (completed).
- Manager, External Relations to check all images sent to other parties in terms of the reproductions guidelines (ongoing).
- Review naming convention of image files to ensure clear labelling of resolution status (end July 2011).
- Create a new risk entry in the NI - General Operations Risk Register that documents the risk of Note Issue contravening its own reproductions guidelines without the prior approval of senior management (end July 2011).

External Relations
Note Issue Department
7 July 2011

INCIDENT REPORT

UNINTENTIONAL DISCLOSURE OF EMAIL ADDRESSES

On 14 July 2011, an email was sent to individuals who had requested an electronic copy of the 2011 numismatic order form. Customers' email addresses were included in the 'CC' field instead of the 'BCC' field, unintentionally making the email addresses visible to all recipients.

Background

NI maintains a database of individuals and businesses wishing to receive copies of the numismatic order form, which is available in physical and electronic formats. Preceding the commencement of a numismatic banknote sale, NI staff send an email with an attached electronic copy of the order form to prospective customers who requested an electronic copy. The email addresses in the database are placed in the 'BCC' field to ensure that email addresses are not made visible to the entire group of recipients.

The Incident

The email, sent on 14 July 2011 in preparation for the 2011 sale, was sent to prospective customers as per accepted procedures. The email addresses, however, were placed in the 'CC' field instead of the 'BCC' field, making the email addresses visible to all of the email recipients. NI Enquiries received two separate emails from customers on the morning of 15 July 2011 advising that, as a result of making the email addresses visible to all recipients, the Bank was in breach of its privacy obligations.

Remedial Action

Upon realising the error, NI staff notified the Manager, External relations, who in turn notified the Head of Note Issue and the Bank's General Counsel. An apologetic email, drafted with the aid of the General Counsel, was sent to the two individuals who commented about the breach of their privacy with the reassurance that administrative procedures that led to this error would be reviewed.

Risk Assessment

The *Privacy Act 1988* prohibits the disclosure of personal information that could identify an individual, without consent of that individual. In this instance, External Relations staff unintentionally disclosed a number of private email addresses. However, an email address alone does not provide sufficient information to allow the identification of an individual. As such, it is not clear if legislation was breached. Notwithstanding the risk of breaching privacy legislation, complaints were received from only two of the 94 email recipients in this case. The Bank's reputation was therefore unlikely to have been adversely affected to any noticeable degree.

Action Plan

Staff have been counseled to take more care when sending emails in future.

Note Issue Department
25 July 2011

RESERVE BANK OF AUSTRALIA

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report by email to 'RM Operational Risk'

Title of Incident Report: Coombs Inventory Discrepancy

Reference Number *(issued by RM upon notification)*: 2011034

Department(s) Compiling the Report: FY

Contact Officer:

Date of Incident	Date Incident Detected	Date RM Notified	Date Report Submitted to RM Operational Risk
16-Jun-11	16-Jun-11	20-Jun-11	26-Jul-11

Summary description of the incident

On Thursday 16 June 2011, the Acting Coombs Administrator, : , completed the May accounts reconciliation and discovered a variance of approximately $2,000 above the Projection 2 figures. It was found that $2,757.25 was paid for replacement linen; delivery of the linen to Coombs confirmed by a despatch docket held by the supplier but there was now no evidence of these items being at Coombs.

Summary of cause

The items were removed from site without authority.

Actual impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational *(Business process/System/Information)* ☑
- Financial ☐
- Legal and Compliance ☐
- Reputational ☐

Description of Actual Impact

The reconciliation of the discrepancy and retrieval of the goods diverted resources from other tasks

Severity of actual impact: Minor

Summary action plan

1. Re-state procedures to ensure staff ordering goods or services can not approve the payment of the subsequent invoice.
2. Reinforce with : staff the importance of maintaining documentation to ensure that all orders are supported by proper authorisation from the Coombs Administrator prior to the order being placed.
3. AD requested to undertake an audit of GL transactions for the previous 3 years to identify any further anomalies.

Estimated Completion Date: 15-Jul-2011

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

FACILITIES MANAGEMENT DEPARTMENT
INCIDENT REPORT FORM

INCIDENT NUMBER:	*47*
RM Incident Number	2011034
ACTUAL IMPACT OF INCIDENT	*Minor*

Coombs Inventory Discrepancy – 16 June 2011

Reporting Officer Name and Contact Details

Senior Manager Property Services –

Incident Description
(Include time, date, sequence of events, names and contact details of those involved)

Summary

On Thursday 16 June 2011, the completed the May accounts reconciliation and discovered a variance of approximately $2,000 above the Projection 2 figures. It was found that $2,757.25 was paid for replacement linen; delivery of the linen to Coombs confirmed by a despatch docket held by the supplier but there was now no evidence of these items being at Coombs.

The Head of FY contacted who advised that had received the goods, they were incorrect and had sent them back to the supplier. The supplier subsequently advised that none of the goods had been returned or exchanged. then confirmed that "had tracked it down", the goods had gone to an old address and would be redirected to the Bank.

The matter was discussed with AG(CS) and RM on Friday 17 June and with the NSW Police by the Head of FY that afternoon.

The goods were returned to the Coombs on Monday 20 June.

The Police attended the Bank to take statements and on Tuesday 21 June, were provided with relevant documentation. On 28 June the NSW Police advised the Bank that the return of the goods would make it difficult to prove They have created a case file and assigned event number to the incident but do not propose to take any further action.

Separately AD were requested to undertake an analysis of relevant GL transactions for the previous 3 years to identify any other anomalies. The AD methodology identified another 33 transactions, all of which were investigated and subsequently found to be legitimate.

Is this potentially a Comcare Reportable Incident? No

Reference to Business Impact Analysis assessment

This incident does not relate to any key processes identified in FY Business Impact Analysis. There are no proposed changes to the Business Impact Analysis as a result of the incident.

Risk Implications

Potential fraud and theft of Bank property.

Existing Risk Treatment Controls (if any)

1. must obtain approval from the before an order for goods or services can be placed.
2. must obtain approval from the before an order for goods or services can be placed.
3. is typically not involved in ordering goods and services, but must approve the order and approve the invoice for payment.
4. A declaration that the account has been checked, goods have been received or work performed and that the account has not previously been paid is provided prior to payment by the .
5. Clear segregation of duties between manager responsible for approving the invoices, and FA Accounts Payable making the payment.
6. Monthly budget reconciliation process includes review of posted transactions and investigation of discrepancies.

Issues:

Unauthorised removal of Bank property from the Coombs Centre.

Proposed Remedial Action

Proposed Risk Treatment Measure	Person Responsible	Deadline	Priority H/M/L
1. Re-state procedures to ensure staff ordering goods or services can not approve the payment of the subsequent invoice.	LG	30 June 2011 Complete	H
2. Reinforce with staff the importance of maintaining documentation to ensure that all orders are supported by proper authorisation from the prior to the order being placed.	LG	30 June 2011 Complete	H
3. AD requested to undertake an audit of GL transactions for the previous 3 years to identify any further anomalies.	AD	15 July 2011 Complete	H

Risk Register Assessment

Remedial Action Item	Corresponding FY Risk Register Item(s)	Changes to Risk Register
1 & 2	F2	nil

Incident report and remedial Action Plan:	
Sighted:	Responsible Manager
Sighted:	Senior Manager (Security)
Sighted:	Head of FY
RM Notified:	Head of FY
Proposed Remedial Action Reviewed:	"Peer" Manager
FY Risk Register Reviewed:	Senior Manager (Security)
Remedial Action Completed:	Responsible Manager
Remedial Action Completed:	"Peer" Manager
Incident "closed":	Head of FY

D11/111108

RESERVE BANK OF AUSTRALIA

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report by email to 'RM Operational Risk'

Title of Incident Report: Targeted Email Virus Attack 17 Nov 2011

Reference Number *(issued by RM upon notification)*: 2011066

Department(s) Compiling the Report: ST

Contact Officer:

Date of Incident	Date Incident Detected	Date RM Notified	Date Report Submitted to RM Operational Risk
17-Nov-11	17-Nov-11	17-Nov-11	30-Nov-11

Summary description of the incident

A targeted malicious email was sent to several Bank staff, including senior management up to Head of Department. The email was purported to be from regarding "Strategic Planning FY2012. The malicious payload was an Internet URL link to a zip file containing a trojan which at the time, was not detectable by the Bank's Anti Virus scanners. The six users that clicked on the link had their PCs isolated until such time the AV vendors could deploy updated virus definitions. By close of business, the definitions were updated and over night virus scans were scheduled. Of note, all of the affected PCs did not have local administrator rights. This prevented the virus from spreading.

Summary of cause

Malicious email was highly targeted, utilising a possibly legitimate external account
It included a legitimate email signature and plausible subject title and content. As the email had no attachments, it bypassed existing security controls, allowing users to potentially access the malicious payload via the Internet.

Actual impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational *(Business process/System/Information)* ☑
- Financial ☐
- Legal and Compliance ☐
- Reputational ☐

Description of Actual Impact

Users with affected PCs were disrupted whilst replacement PCs were organised.
Bank assets could have been potentially compromised, leading to service disruption, information loss and reputation.

Severity of actual impact: Minor

Summary action plan

Deploy updated virus signatures from Completed.
Update email block profile to scan for embedded hyperlinks that host files/applications. - Completed.
Investigate blocking the download of all known executable application file types via the Web Browsing infrastructure. - RMC Feb 2012.

Estimated Completion Date: Feb 2012

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

TARGETED EMAIL VIRUS ATTACK 17-NOV-2011

Risk Management Unit Reference Number: 2011066

1. EXECUTIVE SUMMARY

On Wednesday 16th and Thursday the 17th of November the Bank received suspicious emails purporting to be sent from regarding "Strategic Planning FY2012". The recipient list included several Bank staff, including senior management up to Head of Department. The emails were analysed by ST Security Analysis and found to be malicious in nature.

The malicious payload was found to be a compressed zip file containing an executable malware application. The email had managed to bypass the existing security controls in place for malicious emails by being well written, targeted to specific Bank staff and utilised an embedded hyperlink to the virus payload which differs from the usual attack whereby the virus is attached directly to the email. Of note was that antivirus which is used on Bank workstations and servers did not detect this virus. The issue was escalated to several anti-virus vendors used by the Bank to ensure updated antivirus definitions were created to detect the virus.

It was also found that six users had clicked on the malicious link, potentially compromising their workstations.

ST Head of Department authorised the shutdown of all affected PCs and server until appropriate anti-virus detection and removal capabilities were created. Affected staff were individually notified by ST and FMG Computing. By close of business on the 17th of November, had committed to deploying updated virus definitions that evening. These were released and have been installed at the Bank. All affected PCs have been cleansed and returned to normal operation.

Of note, all of the affected PCs did not have local administrator rights. This prevented the virus in this case, from spreading around the network.

2. SYMPTOMS

- Suspicious email purporting to be from was sent to select Bank staff with a subject heading "Strategic Planning FY2012"
- Email was forwarded to System Security management for further analysis
- Email was found to be linking to a malicious payload on the Internet – subsequent scans revealed the threat was currently undetectable by the workstation antivirus and the server antivirus
- Further analysis showed 6 Bank staff members had potentially opened the malicious payload – these servers were considered compromised and removed from the network

3. IMPACT

- Users with affected PCs were disrupted whilst replacement PCs were organised
- Bank assets could have been potentially compromised, leading to service disruption, information loss and reputation

4. CAUSE

- Malicious email was highly targeted, utilising a possibly legitimate external account purporting to be a senior Bank staff member. It included a legitimate email signature and plausible subject title and content
- As the email had no attachments, it bypassed existing security controls, allowing users to potentially access the malicious payload via the Internet browsing infrastructure

5. ISSUES

- No automatic discovery by the mail filtering software at that time, for these types of malicious emails.
- Workstation and Server assets were potentially exposed as the required virus definitions did not exist for this particular threat
- While users are aware of the need for caution with suspicious attachments, such awareness is unlikely to protect the Bank from credible looking emails and attachments

6. RISKS AND BUSINESS IMPACT ANALYSIS

- STR2005 – Malicious externally generated attack or act of sabotage.

There are no recommended changes to this risk in the risk register. There are also no recommended changes to the BIA ST template.

7. RECOMMENDATIONS

- Deploy updated virus signatures from
- Update the block profile to scan for embedded hyperlinks in emails that link to known applications/executables. Emails that have links to Internet hosted files/application will be automatically blocked and require ST Security review.
- Consider blocking the download of all known application files (including zip files) via the Web Browsing infrastructure. Where necessary, an exception list can be made for specific business units whilst keeping the overall exposure to a minimum.

8. ACTION PLAN

Action Description	Risk	Priority	Estimated Completion Date	Action Assignee
	Low	High	Completed	Security Analysis – ST
Update] email block profile to scan for embedded hyperlinks that host files/applications.	Low	High	Completed	Security Analysis – ST
Investigate blocking the download of all known executable application file types via the Web Browsing infrastructure.	High	Medium	RMC – 1 Feb 2012	Security Analysis - ST

9. DISTRIBUTION LIST

Name	Name	Name

10. SIGN OFF

Title	Name	Signature
ST Department Head		

Reserve Bank of Australia

Risk Management Unit

Incident Report Summary

Please submit Summary and Incident Report to RM Operational Risk

Title of Incident Report

Inadvertent release of internal document related to the tender to an external party

Department(s) Compiling the Report

FA

Contact Officer

Date of Incident

Date Incident Detected

Date RM Initially Notified

Date Report Submitted to RM

Summary description of the incident

The evaluation methodology document for the tender was inadvertently sent via e-mail to an external party who had previously requested a copy of the tender. This occurred when the evaluation methodology was being internally circulated for review and comments.

Summary of cause

Insufficient review of e-mail addresses prior to sending.

Brief description of impact

Please select the relevant impact(s)

- Personnel health and safety ☐
- Operational/System ☐
- Financial ☐
- Legal ☑
- Reputational ☑

Description

This error may have reputational and legal consequences as the probity of tender may be questioned if the Bank had not responded to the error. One component of the tender has been delayed.

Severity of actual impact

Minor

Summary action plan

The recipient of the document has been asked to delete the email, the attachment and any saved copies, and confirm via email that this has been done. The recipient has confirmed the deletion as requested. The section of the tender for which the company was interested in has been withdrawn. Project staff have been reminded of the importance of properly reviewing email addresses. Email groups have been established to ensure that e-mail addresses need not be re-entered each time an e-mail is to be sent to the evaluation committee.

Estimated Completion Date

Note: The Incident Report should include a reference to the risk(s) identified in the Department's risk register.

Is a change to the risk register required as a result of the incident?

- No ☑
- Yes ☐ ▶ Please select
  - Controls ☐
  - Risk Ratings ☐
  - Risk Description ☐
  - New Risk ☐

INCIDENT REPORT

Inadvertent release of internal document to external party on

1. SUMMARY

On a document meant only for internal distribution was accidentally sent to an external party. The document contained the proposed methodology for evaluating the tender. Outlook's auto-complete function included a previously entered email address for a potential bidder. This was not detected before the email was distributed. The external recipient of the email has been contacted and asked to delete the email, the attachment and any saved copies, and the Bank has received an email confirming that this has been done. The specific section of the tender that the external party was interested in has been withdrawn until a later date. Project staff have been reminded of the importance that emails are correctly addressed. Email groups have been created so that there is no need to enter individual email addresses each time an email is to be circulated.

2. DESCRIPTION

The evaluation methodology document was to be internally circulated on Friday, for review and comments on the proposed weightings given to factors for evaluate competing tenders.

The project officer had been responding to requests for the tender documents since the release of the tender on AusTender from an email mailbox specifically established for the project. The evaluation methodology document was sent from the standard work email mailbox. The project officer incorrectly believed Outlook's auto-complete function has separate address lists for each mailbox. It maintains a single list for all boxes. When the project officer entered to send the message to Outlook added an external party to the email instead. The email was sent without the wrong address being detected. As a result the document was inadvertently sent to an external party.

3. CONSEQUENCES

Risk 10 OP/Information/Disclosure in FA's risk register states that the consequences for this type of event are reputational and legal. If action was not undertaken by the Bank the probity of tender could be questioned.

4. RISK REGISTER

Both the Financial Administration and Accounting Operations risk registers address the risk of this kind of event under the Op/Information/Disclosure risk profile.

Reference	Risk Manager	Group	Definition
OPS/Information/Disclosure	Senior Manager AO, Manager AO, Senior Financial Accountant Ops	FA	Reputational – Reputational damage
OPS/Information/Disclosure	FA - Senior Managers AO, AAP, OSF and Staff Payments.	FA	Legal - breach of legislation or policy. Legal action against Bank. Fines and penalties.

5. ACTION PLAN

Action Description	Owner	Estimated Completion Date
Contact external party who received the email and request the deletion of the email and attachments, and any saved copies. Also request an email to attest that this has been done.		Complete
Withdraw the component of the tender until a later date.		Complete
Reiterate to project staff the need to correctly address emails.		Complete
Create email groups for circulation of documents related to the tender and ensure procedures are updated to reflect this as standard in future.		Complete

6. DISTRIBUTION

Assistant Governor (CS)	
Chief Financial Officer	
Senior Manager, AO	
Manager, AO	

7. SIGN OFF

Senior Manager Accounting Operations
(Acting)
Financial Administration