Internal Memo

To: **MD, Director HR, Ag Director ICT, CFO, Director Legal and COSEC**	Date: **17 August 2018**
From: **Forensic Investigator, Electronic Fraud**	Subject: **Vandalized Computers**

1. Background

Pursuant to a whistle-blower report dated 25 July 2018 to National Bank of Kenya ("NBK" or "the Bank"), the Security Department were alerted of a possible case of vandalized computers at the NBK Go-Down Office. Based on the allegation made, the computers which had been used for the Digitization of Account Opening Forms project had been vandalized of their hard drives.

a) The Digitization of Account Opening Forms Project

The Digitization of Account Opening Forms Project was awarded to KODE Network Solutions Limited ("KODE" or "the contractor"), on 1 August 2015 under contract number 013/SKL3/2015. In accordance to the contract, KODE was contracted to supply, install, implement and commission scanning services of the Bank's historical account opening forms into an electronic format to be stored into the Bank's Electronic Document Management System ("EDMS").

The project was run by NBK's ICT Division and the Operations Division. The two divisions were mandated to provide:

- Support/ logistics from the Bank and verify scanned documents;
- Verify the actual number of documents scanned, sorted and filed each day and execute the Daily Summary of the scanned documents;
- Conduct random quality assurance tests and ensure that documents scanned comply with the specifications in the proposal.

The work commenced on 1 August 2015 and stopped on December 2017 when KODE staff abandoned the project and left. From our discussion with Mr James Mwaniki ("Mr Mwaniki"), a KODE supervisor, the last six subcontracted KODE staff came to scan and index documents on the 11 December 2017.[1]

In an email[2] dated 3 November 2015, Mr Thomas Gachie ("Mr Gachie"), requested Mr Mohammed Abdalla ("Abdalla") the ICT Director, to take over the project. Mr Abdalla then sent an email[3] to Mr Emmanuel Wafula ("Mr Wafula") to train a secondary resource Mr Khadija Gamadid ("Ms Khadija") as the Digitization project was fully an ICT project.

Based on this information, we can conclude that the Digitization project is fully under the ICT Division. The Operation Division was to provide the documents to be scanned and house them while they were being scanned.

b) Objectives of the investigation

The Security team accompanied by an NBK IT Officer proceeded to the NBK Go-Down Office to assess the veracity of the allegations. The objectives of the preliminary site visit were as highlighted below:

- Review of the whistle-blower allegation with respect to the vandalized computers; and
- To the extent possible, ascertain the persons culpable.

[1] Appendix 1 - List of Six KODE contracted staff.
[2] Appendix 2 – Email correspondence dated 3 November
[3] Appendix 2 – Email correspondence dated 3 November

2. Findings

Our observations from the physical assessment of the site, interviews and review of documentation, largely, appear to corroborate the whistle-blower's allegations as discussed below.

a) Vandalism of computer equipment

From our assessment of the site with the assistance of Mr Jeremiah Langat ("Mr Langat"), the Facility Manager, we found the following equipment within the room where the project was being undertaken:

Equipment	Ownership	Status
Desktop Computers[4] - 17	NBK - 10 HP	RAM, motherboards and hard-drives extracted - 6
	KODE - 7 Lenovo	RAM only extracted - 5
		RAM and Hard drives extracted - 4
Kodak Scanners - 3	KODE	Intact
Boxes of documents	NBK	Intact

Two of the computers found in the room were not vandalized. However, one had a faulty power supply unit ("PSU") and consequently could not power on.

Below is a breakdown of the equipment vandalized:

Model	Serial Number	Owner	Hard Disk	RAM	Motherboard
HP	CZC141BYOS	NBK	Present	Missing	Present
HP	CZC141BVPX	NBK	Missing	Missing	Present
HP	TRF523ORGG	NBK	Missing	Missing	Missing
HP	CZC141BVMT	NBK	Present	Missing	Present
HP	2UA05109BN	NBK	Present	Missing	Present
HP	CZC152DC6Q	NBK	Present	Missing	Present
HP	TRF5230X31	NBK	Missing	Missing	Missing
HP	CZC141BVRY	NBK	Present	Missing	Present
HP	CZC9512NCK	NBK	Present	Present	Present
HP	TRF5230RFV	NBK	Present	Present	Present
Lenovo	PC0BPF7H	KODE	Missing	Missing	Missing
Lenovo	PC0BPEV2	KODE	Missing	Missing	Missing
Lenovo	PC0BPFDT	KODE	Missing	Missing	Present
Lenovo	PC0BPETE	KODE	Missing	Missing	Present
Lenovo	PC0BPEWR	KODE	Missing	Missing	Present
Lenovo	PC0BPF7F	KODE	Missing	Missing	Missing
Lenovo	PC0BPESD	KODE	Missing	Missing	Missing

From our interviews with the KODE team, they informed us that their last official working day, prior to breaking for Christmas, was 11 December 2017. They confirmed that they had left the computers they had used intact.

[4] Appendix 3 - List of computers.

We, however, see three instances after this date where Mr Mwaniki inconsistently shows up to the Godown office to work on his own. From our review of the security occurrence book, on 15 December 2017, Mr Mwaniki came to work from 11am to 2pm. He came again on 20 December 2017 from 11am to 2 pm and on 21 December 2017 from 12pm to 3pm.

Mr Mwaniki informed us that he was there to index data. From the records of the indexed data, the last data was indexed on 11 December 2017. This contradicts the information provided by Mr Mwaniki.

In addition to this, it came to our attention that prior to the incident being brought to the attention of NBK's senior management, some KODE and NBK staff were aware of the vandalism and had chosen not to escalate the matter to the Security, ICT and Operations Divisions.

From our consultations with Mr Mwaniki and Mr Alexander Madiga, ("Mr Madiga"), the company CEO, informed us that they were aware of the vandalism of the computer equipment at the Godown on 19 July 2018, i.e. the week before the whistleblower alerted NBK management. Mr Mwaniki explained that he had made this discovery when we passed by the Godown to service a scanner as instructed by Mr Madiga. However, he noted that the computer was not powering and when he opened it, he found that several parts had been extracted from it.

He immediately notified Mr Langat, and they proceeded to inspect all the computers and noted majority of the computers had indeed been vandalized. Mr Mwaniki informed Mr Langat that he needed to alert his boss. The following day, Mr Madiga, accompanied by Mr Mwaniki, came to the site to verify the incident that had been escalated to him. He immediately informed Mr Langat that he expected NBK Management to be notified of this and action taken. Mr Langat informed him that he would revert back on this by Friday evening, however, he did not.

Mr Madiga emailed him on 20 June 2018, i.e. the following Monday, requesting for an update, however, Mr Langat did not revert back with this.

It is important to note that during our initial visit to the Godown on 25 July 2018, Mr Langat did not disclose his prior knowledge of the incident and appeared shocked about the vandalism.

Following the interview with the KODE management, we tasked him to explain why he chose to withhold his previous knowledge about the vandalism incident. He informed us that he had decided to do so as he was conducting an internal investigation and was planning escalate the matter to the Security team once he had concluded his investigation.

b) Unreported theft incident

From our discussion with Mr Mwaniki, he informed us that there was a similar incident that had taken place in the course of the project which had not been reported to the NBK Security officials.

He explained that in 2016, an NBK computer monitor had been stolen from the room in which the scanning was taking place. He added that from the review of the CCTV footage conducted with Mr Langat, it showed that a KODE subcontractor had taken the monitor and placed it in his bag.

The incident was reported to Mr Madiga, who took action by ensuring each KODE staff was deducted KES 1000. We cannot ascertain that Mr Madiga reimbursed the bank for the stolen NBK equipment.

According to Clause 3.6(vi) KODE was to insure all equipment provided for this contract. In breach of this clause, we do not see KODE compensating NBK for the loss of the monitor.

We also noted that incident was not escalated to the NBK Security, ICT and Operations Division.

c) Accounts customer relating to the scanned records

From the information provided by the Operations and ICT department, KODE scanned and indexed a total of 7,849,164 account records. The unit cost per image scanned and indexed was KES 2.80 which totaled to KES 21,977,659.20 due for all the works done. KODE was paid a total of KES 20,871,254.80 with a balance of KES 1,106,404.40.

From our analysis[5] of the scanned records log, we noted that there were 15,642 accounts relating to the 7,849,164 scanned and indexed records. Of the records relating to the 15,642 accounts, only records relating to 3,937 accounts were correctly scanned and indexed. The remaining 11,705 had incorrect account numbers.

We also categorized the perceived risk according to the account dormancy status, type of account[6], the Branch. The table below expounds further on this:

N- No Y- Yes

Closed	Count
N	2,723
Y	1,214
Grand Total	**3,937**

Not Closed and Not Dormant	1,075
Not Closed and Dormant	1,648
Grand Total	**2,723**

Dormant Status	Count
Y	2,841
N	1,096
Grand Total	**3,937**

[5] Appendix 4 - Analysis of scanned records
[6] Appendix 5 - List of types of accounts

Branch Code	Number of Accounts
KAKAMEGA BRANCH	3,345
RUIRU	579
NGONG ROAD BRANCH	2
HARAMBEE AVENUE	1
MIGORI -N	1
LIMURU	1
KENYATTA AVENUE	1
EMBU BRANCH	1
NAKURU	1
PORTWAY HOUSE BRANCH - MOMBASA	1
WESTLANDS -N	1
KENYATTA UNIVERSITY BRANCH	1
BUNGOMA	1
KIAMBU BRANCH	1
Grand Total	**3,937**

Furthermore, from our consultations with Mr Mwaniki, he informed us that the scanned customer records were not deleted from the local drives of the computers once the KODE team had uploaded the scans onto the network drive. This confirms that there was sensitive customer information within the stolen drives. This poses a huge risk on data confidentiality of the Bank's customer information.

In accordance to Clause 3.6(iii) within the contract between the Bank and KODE, after scanning, indexing and uploading onto the network, the KODE team was to delete the images from the local drive. However, we do not see this happening. Which leads to possible exposure of the data.

d) Concerns around the project staff

In line with the contract between the Bank and KODE, KODE was mandated to provide three full time designated Employees on site and make available a sufficient number of competent personnel to render the service.

From our discussion with the team on the ground, KODE contracted a total of 30 subcontractors to the project over the contractual period. We were also informed by Mr Mwaniki that there was a high turnover of subcontractors as a result of lack of payment of salaries. He also stated that Mr Madiga was aware of this and did not take any remedial action and attributed his inability to pay them to NBK not paying him. NBK, contrary to the Mr Madiga's allegations, had indeed paid KODE on a regular basis and in accordance to the contract.

Two incidents, which were allegedly attributed to the lack of payment, were brought to our attention:

a) In mid-2017, the KODE subcontractors mobilized and threatened to take all the project computer equipment at the NBK Godown Office as compensation for the non-payment of their dues. Mr Langat and the security team kept the KODE team outside the premise to avoid any damage or loss of the properties.
b) On 13 September 2017, the KODE subcontractors went on strike and did not report back to work until 18 September 2017. In an email dated 13 September 2017, Mr Langat informed Mr Paul Mutai ("Mr Mutai"), the Head of Process and Controls that "*The team are demoralized and lack synergy because they have not received the August payments and on the previous months they had issues on their remuneration. From the*

look of things, it seems the team is on their own and their numbers are reducing day by day. From 35 to 15. Today the kode team did not report to work."[7]

In accordance to clause 3.6(xiv) within the contract, KODE was to secure NBK against any claim by the contractor's personnel on the relevant premises in respect of any loss, cost, expense, injury or claims whatsoever arising from their employment. However, we do not see them do so even after these two incidents, which we can only assume escalated to result in the latest vandalism incident in July 2018.

Mr Mwaniki also informed us that on 23 February 2018, he came to collect one of the project computer's for his personal use, subsequent to being authorized by Mr Madiga. This computer was not formatted to remove scanned images prior to being removed from site. This also posed as a risk.

From our review of the contractor's proposal, they were to be three KODE designated employees on site: Mr Mwaniki (Supervisor), Mr Brian Mrirah (Supervisor) and Ms Anne Ajwang (Indexing Clerk). However, from our discussions with the NBK staff and KODE staff on site, KODE only had one Designated Employee; Mr Mwaniki, to fill in the role of the Supervisor and Indexing clerk. This would suggest that there was inadequate supervision of the sub-contracted staff.

3. Risks identified

We summarise the risks based on our observations as below:

1. A possible exposure of 7,849,164 records relating to 15,642 accounts of NBK Customers Personally Identifiable Information contained within the vandalized equipment. The hard disks contained scans of confidential bank information that could likely land into wrong hands exposing the bank to reputational risk, legal risks and fraud risks.
2. A potential loss of Kes 900K as a result of the vandalism of NBK's 10 computers at the Project site. (* Using the current market value per PC as Kes 90K).
3. We noted that there was a lack of escalation of incidents that took place at the Godown to the NBK Security, ICT and Operations Division. The escalation would have preempted the security team to put in mitigation measures. We believe that the lack of escalation of all the issues at the Godown is what culminated into the vandalism incident.
4. We cannot ascertain if the computer equipment reported to have left or incidents reported at the site are the only ones during the contract period.
5. We observed that there was inadequate access control measures in place in the room where the KODE team worked. There was also no CCTV coverage within that room. As such, we can only speculate what may have happened.
6. We found a number of boxes containing scanned and un-scanned documents were left unsecured within the room in which the KODE staff were working from. We also noted that the room had no access control or CCTV coverage present.
7. From our discussions with the Operations team, we were informed that the staff assigned to the project have since left the Bank and as such we cannot ascertain if a proper handover was done or if the above had been noted.
8. We observed that currently, the staff from the center is not searched while leaving the Premises, but Gate pass is required for any official movement of stuff from the Center. As such it is possible that the

[7] Appendix 6 - Email from Jeremiah to Paul dated 13 September 2017.

individual(s) who vandalized the computers could have walked out of the premise with the equipment and / or Bank records.

4. Recommendations

1. Possible reimbursement of loss of equipment to NBK by KODE in accordance to clause 9 of the contract agreement.

   (Director Legal or Corporate Affairs, Ag Director ICT and Director Operations; Due Date: September 2018)

2. Follow up on legal ramifications where KODE staff absconded duty and terminated their contract without mutual consensus between the two parties which is in breach of contract.

   (Director Legal or Corporate Affairs and Director Operations; Due Date: September 2018)

3. Reconciliation of scanned documents.

   (Ag Director ICT and Director Operations, Chief Finance Officer (CFO); Due Date: September 2018)

4. An audit of payments of KES 20,871,254.80 paid to KODE with respect to the scanned and indexed documents.

   (Action: Chief Finance Officer (CFO), Ag Director ICT, Director Operations; Due Date: Immediately)

5. Pursue possibly suspected staff of KODE or others with possible prosecution if found and or sue KODE for Confidentiality breach.

   (Action: Director Risk (CRO); Due Date: September 2018)

6. The Head of Security and Head of Premises will review and enhance Security at the Go-down within this third quarter.

   (Action: Director Risk (CRO); Due Date: October 2018)

7. We recommend disciplinary action to be taken against the NBK employees found culpable of negligence in their duties.

   (**Action: Director HR; Due Date: Immediately)**

Report prepared by:

Angela Ngava

Brian Osoro

Reviewed by:

Willy Tanui