Audit Scotland Report: Fraud and Irregularity Update 2018/19

College Frauds

Payroll Fraud 1

1. During March 2019, the College was the subject of a payroll fraud that resulted in a payment to a fraudulent bank account.

2. The College believes the fraud resulted from a phishing attack on the home computer of a staff member. This attack allowed the fraudster to obtain the staff member's user name and password to the College email system. The Payroll Department then received an email purportedly from the staff member requesting that their bank account details be amended. As the communication was from a College email address, the request was actioned without reference back to the member of staff. On payment of the March salary, the fraud became apparent when the staff member did not receive their salary.

3. The College has undertaken a review in line with its Fraud Response plan and a report on the fraud has been compiled. A number of actions have been undertaken to address the findings of the report including:

    - Access to the online portal allowing staff to change bank details has been removed.
    - Internal processes have been amended to require secondary verification of changes to bank details.
    - The incident has been reported to the police and both internal and external auditors.
    - The Chair of the Board, Chair of Audit Committee and Chair of Finance and General Purposes Committee have also been informed.
    - Internal audit has been requested to review the amended payroll procedures / policies.

Payroll Fraud 2

4. During May 2019, the College payroll team received an email that appeared to be an internal email from a genuine member of staff, asking the payroll team to update employee bank account details. Had there been a request to change bank details by phone or an external email or letter then checks would have been carried out by calling the employee directly and confirming their pay

reference and national insurance number. This was not done because the changes were requested from an internal staff email.

5. The bank details were updated in the payroll system and used to pay the staff member's salary. After the payroll date, the staff member called the Payroll team to ask why they had received no pay. The Payroll team investigated and established that there had been fraudulent activity. After investigation, it was revealed that the staff email and name were in the display box only and the real source of the email was from an external email address.

6. The Payroll team immediately contacted the College's bank to report the fraud and investigate recovery of the funds. The College bank's Relationship Manager escalated the issue directly to the bank's fraud team. The team also notified the College IT department which blocked the sender email address and reset the email address of the affected employee. The College IT manager also advised the Data Protection team and Information Manager.

7. The College also contacted the receiving bank whose fraud team advised they were already aware that the account was the subject of certain unusual activity. The College also contacted Police Scotland who advised that they would contact the receiving bank directly and establish who set up the account and track down who was involved.

8. Other actions taken by the College include:

   - Fraud seminar at the College (to be delivered by the bank's Relationship Manager) to be arranged.
   - Reminders of warnings of this type of risk have been made to all Finance employees.
   - Update to payroll procedures: with immediate effect, any changes requested by both internal and external email will be subject to the same checks of calling the employee directly and asking them to confirm their payroll reference, national insurance number and new bank details. These checks will be documented and signed by the payroll team. In addition, as part of the month-end payroll checks, the Finance Manager will review these documents.

International Payment Fraud

9. The email accounts of the College International Activity Manager and the College's Chinese Agent ("the Agent") were hijacked by a third party fraudster. Both the International Activity Manager and the Agent received emails on the

same day, supposedly from each other, stating that their email address had changed. Since that point, both were sending/receiving emails to/from the third party fraudster via the purported email address. The third party fraudster would either forward the emails, received through the purported email address, on to the recipient as they were or would amend these slightly. In this way, the general layout and tone of the emails remained the same, which made it difficult for either the International Activity Manager or the Agent to suspect that anything was wrong with the emails.

10. The fraud occurred as a result of an email sent from the Agent about a week later being doctored by the third party fraudster to include a request that the money owed to the Agent be paid to a third party's bank account. The International Manager requested confirmation in writing of the change of bank details. The third party fraudster was able to intercept the email from the Agent which had a copy of the Agent's invoice and letter of confirmation of genuine bank details. The third party fraudster doctored the letter of confirmation to show the fraudulent bank details whilst keeping the genuine company documentation. On receipt of the doctored invoice and the letter of confirmation, the International Activity Manager arranged for a payment to be made to the bank account stated in the letter of confirmation. This was after matching the headed paper, official company stamp and Agent's signature with those held on record.

11. About a week later the International Activity Manager and the Agent had a conversation via "WeChat" and discovered that the payment had not been made to the Agent, that the emails had been intercepted and that they had been conversing with a third party fraudster from 8 January to 22 January 2019.

12. Had the payment been processed through the Purchase Ledger, then normal procedures of requesting both written and verbal confirmation of the change of bank details would have uncovered this. However, as this was an annual payment from the International Office (outwith the Finance Department) the staff involved were not fully aware of the College's Purchasing Procedures and the Bank & Cash Procedures regarding verbal confirmations. Since the incident, the College has strengthened its Purchasing Procedures and Bank & Cash Procedures to apply to all payments, which should help mitigate the risk of this happening again.

13. Actions taken by the College since the fraud was identified include:

- Full internal investigation into the circumstances of the fraud.
- Immediate suspension of all supplier payments until all bank detail changes since 1 August 2018 were subject to additional validation and checks.
- Updated internal procedures in regard to changes to standing data and bank account changes, reflected in updated Fraud Policy.
- Review of internal procedures in regard to changes to email addresses.
- Made staff aware of the incident of fraud and how it could have been avoided.
- Scheduled further fraud prevention training.
- Liaised with the Agent in establishing the circumstances of the fraud.
- Reviewed IT systems for any introduced malware, breach of security or data loss.
- Reported the incident immediately with Action Fraud, Board Chair, SFC, internal / external auditors, College insurers and the police, other relevant Board members and College staff.
- Referred the incident to internal audit for review.