Appendix 3 – Corporate Investigations Case Studies 2022/23

Mandate Fraud

A referral was received from the Head of Transactional Finance, advising that the City had been subjected to a mandate fraud following an email compromise fraud requesting that all payments are now made to an alternative bank account. The fraud had been successful after an employee in the transactional finance team had failed to follow due process and amended the supplier bank account details without independently verifying the change of account request with the supplier by telephone, using known, or open source searched contact details.

The investigation found that an email purporting to be from a supplier in respect of a development project containing an invoice for £575,639 had been received by the Accounts Payable team, it had been shared between staff working in the team for further actions, the email requested a change of bank account data for the supplier. The email communication contained a number of red flags that were missed and should've prevented the change of account being processed, these included the following:

- The letter was titled 'wire instruction letter' – this terminology is uncommon in the UK and should have raised a concern.
- The sort code contains an additional digit and as such would be invalid.
- The language used was poor in places.
- The alleged author of the emails signed off as an Accounts Payable Clerk, working for the supplier and then in later emails had the job title of Chief Financial Officer.
- The supplier landline phone number quoted was a UK mobile number.
- The supplier mobile number quoted was a foreign mobile number, starting in +20, the dialling code for Egypt.
- The date stamp is in a text box.
- The document metadata shows that a programme called PDF Escape has been used to edit the original and legitimate supplier invoice by the imposter to create this change of account letter.
- The email addresses used by the imposters as part of this fraud contained very minor changes to make them appear genuine, these should've been identified on closer inspection.

The Counter Fraud team worked with the Corporate Treasury team to isolate this payment with the City's bank, Lloyds and the receiving bank, HSBC; we also made pre-order enquiries under Proceeds of Crime Act legislation and identified that the full amount was still being held in the receiving HSBC account, and had not yet been moved; we ensured that a fraud marker was placed on this account and credit whilst liaison with Lloyds continued and requested that the payment was frozen by HSBC and any movement could potentially be treated as money laundering.

The matter was reported to the City of London Police who undertook a criminal investigation with the support of the City's Counter Fraud Team. The investigation found that the imposter had set-up new internet domains to appear to look like the supplier; IP data was scrutinised, and this identified that the fraud was perpetrated in the USA. Owing to the fact that the City had successfully frozen the funds and was arranging recovery, and that the perpetrators were

in the USA and outside of Police jurisdiction, the Police closed their case with no further action.

The payment made was recovered in full, and following conclusion of this investigation a new protocol for the treatment of financial loss resulting from bank mandate fraud has been produced and deals with incidents of this nature. This protocol has been agreed between key stakeholders and sets-out the process for responding to mandate frauds impacting the City of London, across all of its funds, and how any losses suffered as a direct result of such fraud will be covered.

Similarly, revised terms and conditions for suppliers and contractors have now been implemented by City Procurement, following engagement with the Comptroller and City Solicitor. An electronic communications clause has been added to the official order form for all new suppliers and contractors, with each party being responsible for maintaining the integrity and security of its own data storage and transmission systems, taking into consideration current applicable guidance issued by the National Cyber Security Centre ("NCSC").

Agency Staff Multiple Contract Fraud

A referral was received from a CoL manager, following contact with another public sector organisation alleging fraud with an agency staff member. The agency worker, who was a professionally qualified professional and working on a contract basis for the City of London since December 2021, applied for a placement in a professional role with the other organisation in July 2022. The CV she supplied to the employment agency falsely stated that her CoL placement was coming to an end at the end of July 2022. Despite a manager at the other organisation wishing to interview her in person she was only available for a Teams interview, which was consistent with a lunch break.

Her placement with the other organisation commenced in August 2022 and most contact was online via Teams. The agency worker only attended the office three times, saying she was unable to attend due to childcare.

The agency worker continued with her placement with the CoL, and this was discovered after a phone call between her manager and a counterpart at CoL. She was expected to work similar core office hours at both organisations. The workers placement at both organisations we terminated in November last year.

The worker had been submitting weekly online time sheets stating that she had completed 37 or 37.5 hours' work for the other organisation The hourly rate paid was £92.07. The total amount paid to the agency by the other organisation totalled £30,153. During this period, she submitted timesheets claiming to have worked 4 or 5 full days each week for CoL at a similar hourly rate, and £25,022 was paid to the agency.

In both organisations the worker held a position of responsibility for public funds and had access to financial systems. The worker attempted to mask the multiple working contracts by working for the other organisation under a Ltd Company basis.

Appendix 3 – Corporate Investigations Case Studies 2022/23

The matter was reported to Action Fraud, who are taking no further action, it was further reported to the workers professional body who are investigating the complaint made about the fraud.

If the fraud had gone undiscovered the annual earnings across both contracts would have been worth over £215,000.

Misuse of Addison Lee Account for Personal Gain

This mater was referred to the Counter Fraud Investigation team by colleagues in the Town Clerks Business Management team who had been reviewing the journeys billed against the City's Addison Lee account as part of the pan-London response to the Covid Pandemic.

The City opened up its Addison Lee account to employees of partnership organisations to ensure that they could safely get to and thro the pan-London response HQ during the pandemic. Upon review of the journeys, it was identified that a high number of journeys had allegedly been made by an employee at Camden Council; we worked with colleagues in Camden's Counter Fraud Team who engaged with the employee who denied that they had made the journeys. Further investigation found that this employee had been subject of an attempt to frame them with the journeys by a former Camden employee who had fallen out with the worker when they both worked together.

Working with Addison Lee we identified detailed journey data, IP data and telephone contact data and established the owner of the device used to book and make the journeys through regulated enquiries with communication providers under the Regulation of Investigatory Powers Act. We further found that the destination address was very close to the individuals home address providing further evidence to support our investigation. A full examination of journey data found that a total of £739.50 was fraudulently spent on journeys by the employee who was interviewed under caution by colleagues from the City of London Police.

The employee was eventually charged with Fraud by False Representation under the Fraud Act 2006 and pleaded guilty at Westminster Magistrates Court to the offences at the first opportunity, the defendant was sentenced on the same day and ordered to repay the City in full in compensation for the misuse of the Addison Lee account and was fined a total of £1,117.50. The compensation has since been repaid in full to the City of London.

Tighter controls have since been implemented around the booking of journeys on the City's Addison Lee account.