Appendix 10: Counter-fraud and Corruption Q3 Summary

Fraud investigation

During Q3, six new cases were opened (2020/21 Q3: two new cases) and four cases were closed. Of the six newly opened cases, two cases involved allegations of fraud within procurement and supply chain activities and one case involved an attempted payment diversion fraud committed against TfL by an unknown third party. Two financial investigations were conducted involving two subjects and three bank accounts. One Suspicious Activity Report (SAR) checks were undertaken during the quarter. The Counter-fraud and Corruption (CFC) team also undertook investigations into 50 miscellaneous referrals during the quarter.

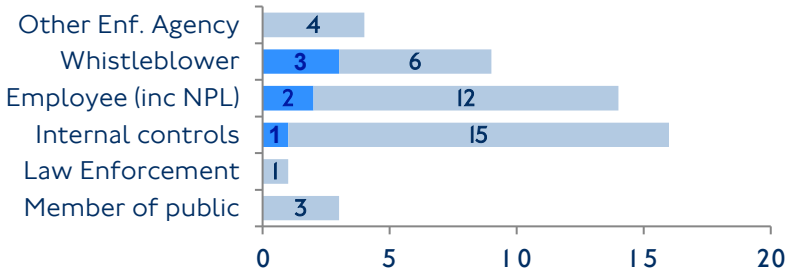
Fraud prevention

- The CFC team hosted their annual Fraud Awareness Week remotely, which took place in conjunction with National Fraud Awareness Week. To raise awareness of fraud, the CFC team worked with the Comms Team to produce a 'click-bait' intranet article and separate holiday fraud bulletin that resulted in over 3,800 views. Other activities included daily Yammer 'Did you know' posts from the Head of CFC on fraud related topics, fraud awareness presentations on digital screens in our main office buildings, a digital desktop advertisement about reporting fraud and a short video highlighting the work of the CFC team and notable recent convictions.

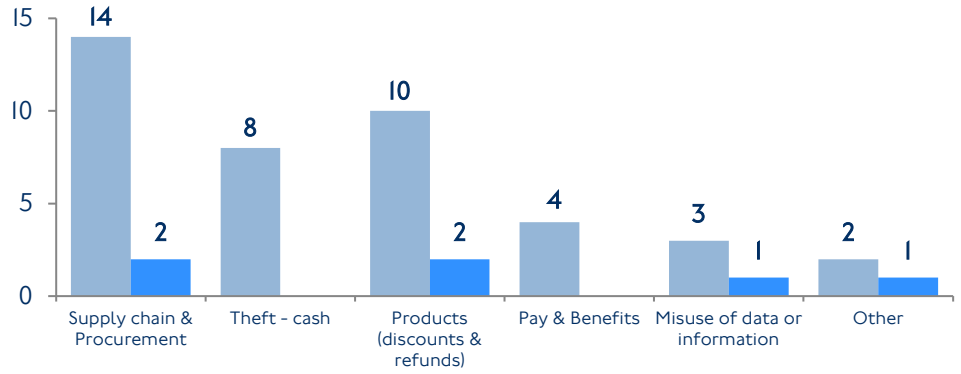
Cases by directorate

Investigations	B/F	New	Closed	C/F
LU	22	3	1	24
Surface Transport	4	0	1	3
CCT	7	0	1	6
Crossrail	3	0	0	3
Major Projects	1	0	1	0
Commercial Dev.	1	0	0	1
General Counsel	2	2	0	4
Human Resources	1	0	0	1
Finance	0	1	0	1
Total	**41**	**6**	**4**	**43**

Cases by source New and Brought Forward



Cases by type New and Brought Forward



Significant closed cases

Case 21-910 Allegation of TfL email account compromise and attempted payment fraud

A senior employee's TfL email account was compromised and an attempt made to obtain payment on a fraudulent invoice, valued at £148,600. The Cyber Security team confirmed that the senior employee's account details were likely compromised through 'credential stuffing' or a 'phishing' email. The CFC team identified that two fraudulent emails were sent from the senior employee's account in the early afternoon of 16 September 2021, the first to Accounts Payable, requesting payment on the fraudulent invoice and the second an hour later, confirming the urgency of payment. Following receipt of this second email, fraud was suspected and confirmation was obtained from the senior employee that he had not sent either email. No payments were made. The incident was reported to Action Fraud. No suspects have been identified. The Cyber Security team reported that a misconfiguration in suspicious login detection has been discovered and corrected, meaning that Cyber Security Operations should now be notified of this type of attack in the future. This case is now closed.