Appendix 11: Counter-fraud and Corruption Q3 Summary

Fraud investigation

During Q3, five new cases were opened, and three cases were closed. The five new cases included an attempted payment diversion fraud linked to an email account compromise at the Greater London Authority (GLA) (see significant closed cases below), an allegation of overtime fraud and an allegation of a conflict of interest within Procurement.

Fraud prevention

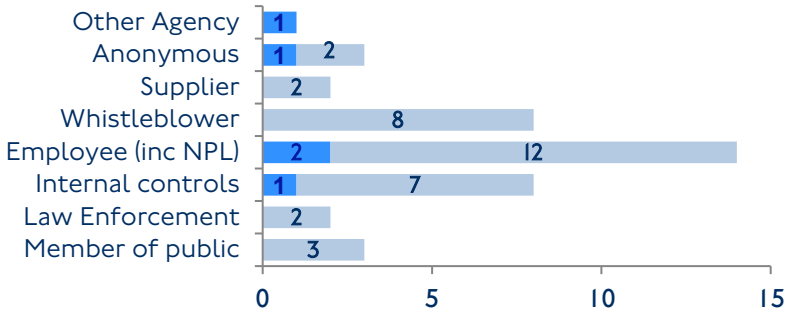
- Members of the Counter-fraud and Corruption (CFC) team attended the quarterly Professional Services Procurement & Commercial (P&C) event, hosted by senior management from the business area. The CFC team presented to small groups about the role they performed and the risk of fraud within end-to-end procurement processes. This was followed by question-and-answer sessions. Over 100 P&C colleagues attended the event and received the presentation.
- The CFC Steering Group met remotely in October 2022. The group, that has recently undergone a review of membership based upon fraud risk within TfL, heard general fraud risk updates from a number of new members including Customer Contact Operations and London Underground Operations. The Head of CFC provided his regular update about new and ongoing fraud investigations.

Cases by Chief Office

Investigations	B/F	New	Closed	C/F
Operations	24	4	1	27
Customer & Strategy	9	0	1	8
People	1	0	0	1
General Counsel	1	0	0	1
Capital	0	0	0	0
Finance	1	1	1	1
Total	**36**	**5**	**3**	**38**

Cases by type New and Brought Forward

Cases by source New and Brought Forward



Significant closed cases

Case 22-914 Allegation of attempted payment diversion fraud

In November 2022, it was reported that several GLA email accounts had been hacked. As a result, a TfL employee received a series of fraudulent emails, purportedly from a GLA employee, requesting changes to bank account details to divert invoice payments totalling £3.8m. The payments had already been correctly made prior to the emails being received, so no money was lost. In addition, several other phishing emails were sent to various TfL employees from compromised GLA accounts, although TfL's Cyber Security team were able to successfully block the malicious link contained within it. From analysis of hacked accounts and the emails sent, the source of the hack is believed to be outside the UK. No suspects have been identified. The GLA has reported the incident to Action Fraud and TfL has made a similar report with regards to the attempted fraud. Some control environment concerns have been discussed with senior management in Business Services, who will take necessary action. This case is now closed.