

## Appendix 2 – Corporate Investigations Summary

Nature of Concern	Investigation/Outcome Summary	Value (£)
Mandate Fraud	<p>Following routine chasing of invoices at year end, the City received an email from a supplier with two invoices and amended bank account details. The change of account request was processed, and the invoices paid. Concerns were raised when the supplier enquired about payment and when advised of the account the payments were made to the supplier claimed to not have any knowledge of the account or the request to amend the bank account.</p> <p>During our investigation we reviewed the background of the reported fraud, analysed the internal documentation and correspondence and liaised with key internal stakeholders; we found that all email communication had been received from the suppliers recognised email accounts and although the City had not telephoned the supplier to verify the change of account, reasonable actions were taken to verify the validity of the request and we concluded that the City had not been a victim of this fraud, nor should it be liable for any error as the payment was made to the supplier in good faith.</p> <p>Our investigation identified that there were opportunities missed that may have helped to identify this fraud and these were reported to management along with three recommendations to improve the control environment and mitigate future risks, all of which have been accepted and are being implemented.</p>	27,735
Mandate Fraud	<p>Concerns were raised when Payroll colleagues identified that the email account of a supplier may have been compromised resulting in a request to amend bank account details being received and processed.</p> <p>During our investigation we reviewed the background of the alleged fraud, analysed email correspondence and liaised with the supplier, who confirmed that they had been subject to a cyber-attack.</p> <p>It was found that the City had been a victim of this fraud and that some employee records held by the supplier and used to process the services delivered may have been compromised – this was reported to the City's Information Team.</p> <p>Our investigation identified the owner of the account that the monies were paid in to and these, along with the details of the fraud and our internal investigation were reported to the Police who are undertaking a criminal investigation.</p> <p>The investigation identified that there were opportunities missed that may have helped to identify this fraud and these were reported to management along with four recommendations to improve the control environment and mitigate future risks, all of which have been accepted and are being implemented.</p> <p>We are working with the City's Risk &amp; Insurance Manager to recover the losses associated with this fraud.</p>	8,043
Fraudulent application of discretionary	<p>A report was received from the City's Housing Benefits Team regarding two applications for discretionary housing payments. The applications were reviewed and found to have been completed by the same person, with counterfeit supporting evidence provided identified through a review of the metadata within the documents. Although the</p>	1,700

housing payment	<p>applications were allegedly made by different people it was found that the National Insurance Numbers on the applications did not match official records when checked and the telephone numbers provided on both applications were the same. The applicant was advised that a verification visit to the address listed on the applications would be made and when attempted there was no response. Checks against Council Tax records also identified discrepancies with the information provided on the applications.</p> <p>A decision was made not to award discretionary housing payments on the basis of the concerns identified and the applicant(s) was informed of this decision. No appeal was made against this decision.</p>	
--------------------	--	--