

# Monthly Threat Update - MTU

## Public – December 2023

Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1<sup>st</sup> – 30<sup>th</sup> November 2023. Please note that all information and data included in the Crime Trends Summary and Current Reporting Trends was true as of **20<sup>th</sup> December 2023**.

**Contact:** If anyone has any information they wish to put forward to be considered for this document, please contact the Strategic Research and Analysis team on: [StrategicResearchandAnalysis@cityoflondon.police.uk](mailto:StrategicResearchandAnalysis@cityoflondon.police.uk)






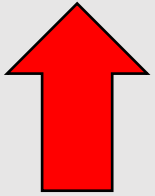
### Contents:

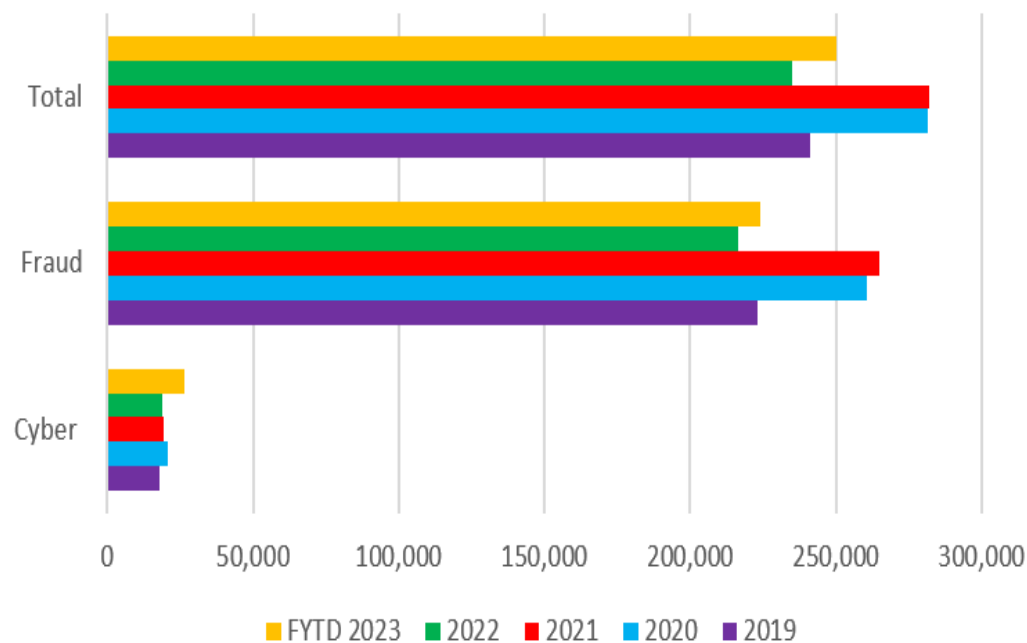
- [Crime Trends Summary](#)
- [Current Reporting Trends](#)
- [Horizon Scanning – Emerging Issues & Threats, Monitoring](#)
- [Distribution List](#)



# Current Trends Summary

## Action Fraud Crime Reporting Volumes in November 2023

	Report	Direction
 <p>Total</p>	<p>32,837</p> <p>3%</p>	
 <p>Fraud</p>	<p>28,862</p> <p>2%</p>	
 <p>Cyber</p>	<p>3,975</p> <p>7%</p>	



**Total losses** for crime reports, which have been verified, have shown an overall decrease this month, by 10%, from **£161 million** in October to **£144 million** this month. Verified losses, for November, are 7% above the previous year average monthly loss of £135 million.

When breaking down financial losses, **fraud offence** losses saw a **decrease of 11%** when compared to the previous month, however, **cyber offence losses** saw a significant **increase of 58%**.

**Both crime and information reports received for fraud and cyber** have shown an increase, by 2%, in November, from 48,518 in October, to 49,306 this month.

Crime reporting relates to reports where there has been a loss, whereas information reports relate to cases where fraud could have occurred but did not.

**Explanation of Figures:** The columns above on the left show the crime reports (excluding information reports) received for November 2023 and the percentage change from the previous month, broken down by all reports, fraud reports and cybercrime reports. The graph on the right-hand side shows the Action Fraud crime reports received for each financial year to date, broken down by all reports, fraud reports and cyber reports.



## Current Reporting Trends (Crime & Info)

RAG ratings are indicative of reporting trends for this month, in comparison to previous month figures. *Green boxes* illustrate a *decrease* in reports, *amber boxes* are indicative of *no change* and *red boxes* highlight an *increase*.

Fraud Type	RAG	Percentile Shift (in comparison to the previous month)	Comments
Romance Fraud	Green	9%	Following an increase last month, November figures have dropped by 9%, when compared to the previous month average. Overall, figures are still significantly above the previous year average, by 58%.
Courier Fraud	Red	18%	There has been a continual increase for courier fraud reporting, and this month is no different as we see a further 18% rise for November. Reporting volumes remain relatively low and larger percentile shifts can be attributed to this.
Cheque, Plastic and Online Bank Accounts Fraud	Red	2%	This fraud type has previously shown a general monthly increase since April 2023, with the exception of September reporting. This month has followed trends and shown a further increase by 2%. Reports are relatively high, at 5,691, and are close to the peak volumes seen at the beginning of the year, in Jan 2023, at 5,911.
Hacking – Social Media and Email	Red	9%	This month has shown an increase of 9% for this fraud type and Hacking - Social Media and Email remains relatively high in volume. Reports for November have reached 2,659 and now sit 252% above the previous year average.
Other Financial Investment	Green	8%	Other Financial Investment fraud reporting has decreased by 8% in November. This fraud type remains higher than the previous year average, by 59%.
Fraud by Abuse of Position of Trust	Red	1%	There has been a continued increase in November, for Fraud by Abuse of Position of Trust. Notably, due to the low reporting volumes for this fraud type, the 1% rise is reflective of an increase of two reports, from 317 to 319, when compared to October.



## Current Reporting Trends (Crime & Info) Cont.

RAG ratings are indicative of reporting trends for this month, in comparison to previous month figures. *Green boxes* illustrate a *decrease* in reports, *amber boxes* are indicative of *no change* and *red boxes* highlight an *increase*.

Fraud Type	RAG	Percentile Shift (in comparison to the previous month)	Comments
Online Shopping and Auctions		5%	Interestingly, at a time when consumers are likely to increase online shopping habits, we have seen a decrease in reporting levels for Online Shopping and Auction fraud by 5%. It is unknown at this stage as to why there has been a decrease, nonetheless, volumes remain relatively high; just over 5,500.

### So What?

Overall, November has not shown any significant shifts in reporting trends for the listed fraud types. Those that have larger percentile shifts can be attributed to lower reporting volumes.

Online Shopping and Auction fraud, whilst noting a 5% decrease in November, will be monitored going forward due to concerns of a predicted rise in the weeks to come. This would be in line with an increase in online consumerism over the December period, particularly Boxing Day sales, where opportunistic threat actors may look to exploit unsuspecting victims with deals a little too good to be true.



## Emerging MOs of Interest

### Package Delivery

Phishing emails are currently being circulated regarding delivery of packages. The body of the email states that the recipient has one package out for delivery and a code is provided for them to track and/or schedule delivery of the item. Underneath an image of a parcel, there is a link titled "schedule your delivery". It is believed that this link is designed to harvest personal and/or financial information, along with a potential download of malicious malware. It would appear that the email attempts to emulate branding colours and styles of Royal Mail, adding to perceived legitimacy of the content. With an increase in online shopping habits around the Christmas period, it is likely that many more individuals are expecting the arrival of parcels and may therefore be more susceptible to this scam.

*City of London Police, NFIB, Cyber Intelligence, Dec 2023*

### Temu Tricks

Phishing emails have been distributed advising recipients that they have 'won' a Temu pallet or mystery box. Some of the fraudulent emails request that the recipient complete a survey in order to claim their prize: a 'pallet of items'. In addition, a majority of the emails request that the victim provide card details to cover a small postage fee. The victim is subsequently signed up to automated schemes where they are charged a certain amount per month. The links included within the main body of the email are believed to be malicious; either to harvest personal and financial information or to download malware onto the victim's device. The emails make use of Temu branding in order to deceive the recipient into believing they are genuine. In less than a month (09<sup>th</sup> Nov – 23<sup>rd</sup> Nov) Action Fraud has received just under 19,000 reports for scams relating to the above.

*City of London Police, NFIB, Cyber Intelligence, Dec 2023*



## Cost-of-Living Crisis Update

# 53

Relevant reports

### Increase (194%)

*\*when compared to previous month figures.*

*Caveat: search terms were expanded this month, which may account for the large percentile increase in relevant reports*



### Reporting Breakdown

Relevance to cost-of-living	Reporting
Phishing, Vishing, or Smishing	15
Fraudulent support claim	14
Increased impact of fraud	9
Contributing to victimisation	7
Domestic fraud	5
Postal fraud	3
<b>Total</b>	<b>53</b>

#### Notable MOs:

- Postal fraud reports where the recipient is asked to access a QR code on the letter and enter personally identifiable information (PII). This is based on an **offer of a discounted water bill from Thames Water**. It is not a genuine letter and Thames Water have commented on this publicly.
- In October there were zero reports identified as instances of **fraudulent claims for cost-of-living support payments**. **In November there were 14**. This is not surprising as the payments were rolled out at the end of October into mid-November. The 14 reports also include **instances of frauds targeting the Warm Home Discount scheme**.
- The **Phishing, Vishing, and Smishing reports** were all **instances where the recipient was offered a grant or discount related to the cost-of-living**, such as a payment from the DWP or a discount from their energy supplier. These social engineering attacks aim to gather PII from the victim to be used to commit fraud.

**SERS: An additional keyword search was completed on SERS (suspicious email reporting service).** From 01/11/23 to 30/11/23.

- The most **commonly reported phishing emails** linked to the cost-of-living were emails **offering discounts on electricity (341 reports) and energy (147) bills**. Six reports offered water bill discounts. Notably, there were no reports identified as naming Ofgem.
- **23 reports were received which mentioned DWP**, but there was no one most prominent MO within these reports.
- Seven reports directly named the cost-of-living, but again there was not a standout MO within these.



## Distribution List

Protective Marking	PUBLIC
FOIA Exemption	No
Suitable for Publication Scheme	No
Version	Final
Purpose	CoLP Strategic R&A Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.
Owner	CoLP
Author	Strategic R&A
Reviewed By	Senior Analyst Strategic R&A

Copyright © City of London Police 2021 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this Alert, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this Alert, please contact the City of London Police. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

