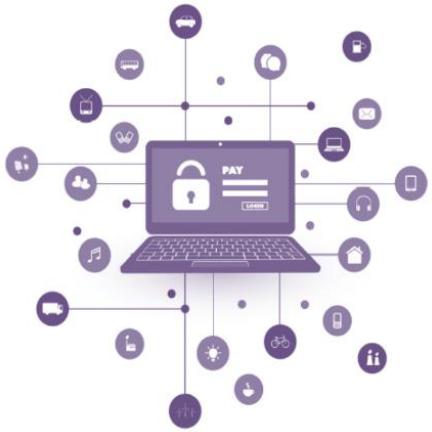
Monthly Threat Update - MTU Public– June 2022

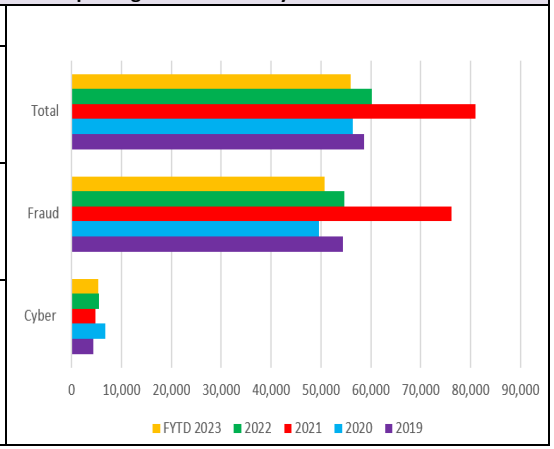
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1st – 31st May 2023.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in May 2022		
	Report	**Direction**
Total	28,782 **4%**	↑
Fraud	25,805 **2%**	↑
Cyber	2,997 **29%**	↑



Explanation of Figures: The columns above on the left show the crime reports (excluding information reports) received for May 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.

- **Total losses** for crime reports, which have been verified, have showed a increase in May, by 80%, from **£140 million** in April to **£252 million** this month. Verified losses, for May are 1% below the previous year average of £255 million.

- **Both crime and information reports received for fraud and cyber**[1] have shown an increase in May from 40, 698 (April) to 42,876.

[1] 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.

Fraud Type	RAG	Percentile Shift (in comparison to the previous month)	Comments
Dating Fraud		**1%**	Reporting this month has shown a slight increase by 1%. Reports for May are at 673 and sit 32% above the previous year average.
Mandate Fraud		**29%**	Following a decrease last month, figures for this fraud type have begun to rise again, however, they remain lower than the spike seen in January 2023.
Courier Fraud		**9%**	An increase is seen in this months' figures, however, reporting levels remain relatively low with only 70 reports being received for the month of May.
Cheque, Plastic and Online Bank Accounts Fraud		**3%**	There has been an increase in this fraud type and reporting levels are now just above 5,000. However, figures remain below

			those seen in the spike of January 2023, which showed 5,911 reports.
Computer Virus and Malware Fraud		**7%**	Reports have risen by 7% this month, however, the figures are relatively low and on average it is 18% lower than the previous year.
Computer Software Service Fraud		**8%**	Following a decrease last month, the volume of reporting for this area has continued to drop. Current data shows that this fraud type remains 31% above the previous year average.
Application Fraud		**5%**	After a decrease in last months' (April) figures, an increase has been noted of 5% this month. This takes the total number of reports to 6,777.
Hacking – Social Media and Email		**43%**	Reports have spiked this month by a substantial 43%.
Online Shopping and Auctions		**5%**	Mays figures have followed last month's decline, falling by a further 5%. Reports remain high for this crime type (5,532 for May). The ongoing cost-of-living crisis will continue to exasperate this shopping habit, whereby consumers look around for "good deals", and as a result consumers become vulnerable to these types of scams.
Retail Fraud		**109%**	The largest increase, for May, has been seen in the reporting volumes for retail fraud. Figures jumped from 164 (April) to 343 (May).
Other Financial Investment		**7%**	Other financial investment fraud has risen by 7% this month, from 1,190 reports received in April to 1,270 received in May.
Fraud by Abuse of Position of Trust		**15%**	Another increase witnessed for this fraud type, however, reporting level remain relatively low.

Current Reporting Trends

March MO's

Malicious Mortgages: Reports have been received for potentially malicious emails relating to mortgage offers. Many of these emails are offering low rates/reduced monthly payments. The content of these emails contain links for a 'personalised quote', professional looking colour schemes, logos and banners. Some also contain time limits such as 'this offer will expire in 24 hours, prompting recipients to act more impulsively without taking time to consider the authenticity of the email. Another tactic employed by threat actors is to entice recipients by using lines such 'this will only take a minute', encouraging potential victims to engage as they feel they can potentially save a large amount of money in relatively short period of time. The current climate, where many people are concerned about the elevated interest rates, the offer of a reduced mortgage/lower payments may seem too good to resist[2].

Gifting Scams: a recent MO from fraudsters is to attempt to lure victims in with phishing emails congratulating them on winning a bottle of perfume (specifically J'Adore) or a gift card. The recipient is encouraged to click on a malicious link, designed to harvest their personal and/or financial information.[3]

Fake Job Offers: reports received of a new MO relating to fictious employment opportunities. Potential victims are receiving messages via WhatsApp informing them of a job opportunity and in order to progress this, all the recipient is required to do is to reply so that their details can be passed on to "HR". Following this engagement, the victim receives a text from the threat actor, claiming to be from HR, advising the recipient that they will be sent a phone for work purposes and that they are required to log onto the device in order for it to work. Once the phone arrives, the scammer advises the victim on how to set it up. This includes asking them to log into their online banking so that they may pay the wages into that account. After harvesting this information, the suspect then removes money from this account and ceases further contact with the victim[4].

Employment Scam: reports have been received that suspects are potentially compromising/exploiting agency applications. Of particular note is an MO linked to a carer. The carer was contacted by the suspect via their work app and asked whether they were available for consultation. When the carer informed them that they were not available at this time, the suspect proceeded to offer the carer a job opportunity elsewhere, with additional benefits. They then requested that the victim contact them via WhatsApp in order to take part in a security check for the new role. This security check was supposedly more detailed than the victims existing DBS clearance. The victim was sent a link for the security check. The victim was subsequently asked for card details and OTP from the bank by the suspect.[5]

Protective Marking	PUBLIC
FOIA Exemption	No
Suitable for Publication Scheme	No
Version	Final
	CoLP Strategic R&A

[2] City of London Police, NFIB, Cyber Intelligence Unit
[3] City of London Police, NFIB, Cyber Intelligence Unit
[4] City of London Police, NFIB, Serious and Complex Case Team
[5] City of London Police, NFIB, Serious and Complex Case Team

Purpose	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