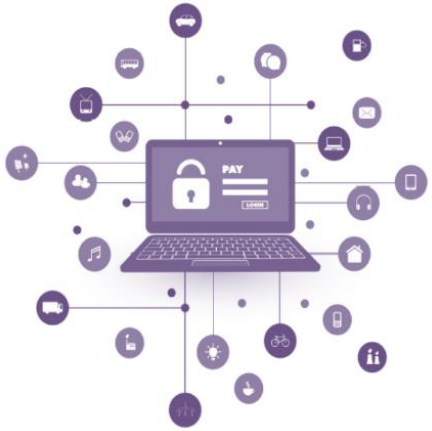
Monthly Threat Update - MTU Public– June 2022

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 2022.

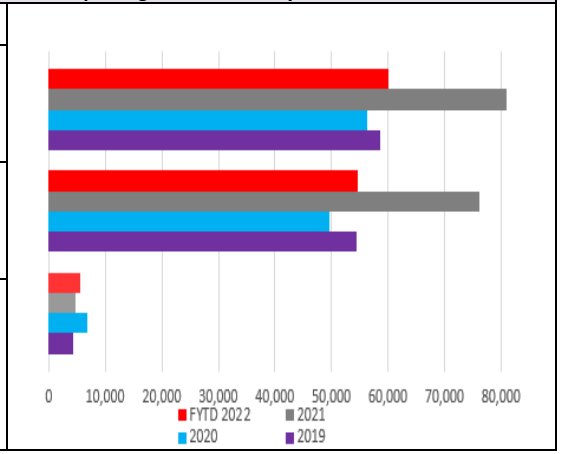


Contents:

- Crime Trends Summary
- Current Reporting Trends
- Horizon Scanning – Emerging Issues & Threats
- Distribution List

Crime Trends Summary

Action Fraud Crime Reporting Volumes in May 2022		
	Reports	Direction
Total	31,313 **8%**	↑
Fraud	28,573 **9%**	↑
Cyber	2,740 **-2%**	↓



Explanation of Figures: The columns above on the left show the crime reports (excluding information reports) received for May 2022 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.

- Fraud and cybercrime reports to Action Fraud have risen in May by 8% to 31,313.

- When looking at the financial year to date (April – May 2022) as shown in the graph, reporting figures overall are significantly below the same period in 2021 for fraud (during covid restrictions), however, the reporting volumes are more than they were during the same period in 2019 and 2020. This pattern is also shown when looking at fraud reporting specifically. When examining cybercrime reporting, the figures show that reporting is higher in the financial year to date compared to 2021 and 2019 but are below the figures for the same period in 2020. These comparisons to previous years will continue to be examined in subsequent MTU's.

- **Total losses** for crime reports, which have been verified, dropped in May from **£359 million to £193.5 million.** This is below the previous year average of £207.5 million.

- **Both crime and information reports received for fraud and cyber**[1] have slightly increased in May from 41,591 to 44,810. For both crime and information reports, 30 out of 54 fraud types showed an increase in reporting compared to the previous month, whilst 22 out of 54 fraud types showed an increase in reporting compared to the same time last year.

- **Whilst fraud has increased, cyber-crime and information reporting** has dropped for the second month in a row by 2% however, it is still 12% higher than 2021 average. Apart from small increases in Computer Viruses, Hacking (Extortion), Denial-of-Service Attacks and Computer Hacking - PBX/Dial Through, all other cyber types show a drop in reporting in April. Hacking – social media and email continues to remain the most prolific cyber-crime type.

[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.

- **Telecoms Industry Fraud (crime and information) has increased again from last month where it was reported that reports have been steadily increasing,** with some slight variants, from a low in April 2020. Reporting remains at the highest since February 2019.

- **Lender Loan fraud** (crime and information reports) have increased in May to the highest reporting since March 2021. Reporting is still lower than pre-pandemic though. This fraud is predicted to rise due to the cost-of-living crisis.

- **Online Shopping and Auction fraud** (crime and information reports) has dropped to the lowest levels since March 2020, which is when the lockdown first took place. Figures have been steadily going down since a high reporting level in January 2021 and are now like pre-pandemic levels.

- **Ticket Fraud** has been steadily increasing since restrictions were eased and events have opened once more. Reporting has increased from last month and as many big events are taking place over the summer months, this will be one to monitor.

- **Investment Fraud:** Other Financial Investment reporting has increased in May by 8%. Reporting is now 2% below the previous year average. Shares Sales have also increased by 3% after a large drop in reporting in the previous month and Pyramid and Ponzi schemes have jumped by 25% from the previous month, reporting is now up 55% from last year average. Share sales figures are slightly higher than pre-pandemic. Pyramid and Ponzi and Other Investment are higher than pre-pandemic.

- **Dating Fraud:** Both crime and information reporting increased for the second month in a row from 682 reports in April to 777 reports in May.

Current Reporting Trends

May MO's

- A high number of reports are still being received in May in relation to numerous websites advertising tax rebates. As at the end of May, 400 reports had been received about fake tax refund emails. One company has been reported over 100 times in May. According to reports, this company had collected tax rebates from HMRC on behalf of several individuals, having received legal documents along with their signatures stating that they can be paid on their behalf.

- Reports continue to be received from people who are looking to renew their driving licence online and are directed to a fraudulent website, which requests personal and financial information.

- Victims reported receiving a text message claiming to be from the NHS stating the recipient had been in close contact with someone with Omnicron and they needed to book a test. The message provides a link where the recipient can book the test, the recipient is directed to a site that looks like the NHS website. The recipient inputs personal information and financial information as the website states they must pay a delivery charge for the test. Although this is not a new MO, with the rise in covid cases we would expect to see more of these reports over the coming months.

- Action Fraud are still receiving a high number of reports relating to text messages stating that a delivery has been attempted but the recipient was not home. To reschedule a new delivery date the recipient is asked to click on a link which takes them to a website requesting personal and financial information. There have been

previous variants of this type of message, including requests for payments of customs fees.

- Reports have been received from victims in relation to the purchase of kitchen equipment online. The victims received email confirmation of the orders and money was taken from the victims' accounts, but no purchases have been received.

- Action Fraud have issued an alert warning people to watch out for fake Tesco emails about gift card giveaways. The email state that the recipient has been selected for the chance to win a £500 Tesco gift card. The links provided in the email lead to phishing websites that are designed to steal your personal and financial information. When the alert was issued, Action Fraud had received 172 reports so far.

- Action Fraud and other agencies have issued several warnings stating that scammers are sending text messages appearing to be from Ofgem offering rebates. As of 25th May, over 750 reports had been received in just four days in relation to these scams.

- Action Fraud have also issued alerts around both ticket and holiday fraud. These areas have been mentioned in previous MTU's as emerging threats and we would expect to see reporting rising over the coming months.

Horizon Scanning – Emerging Issues & Threats

Student Scams

Over the summer holidays, many students will be looking for jobs to support their studies and accommodation to live in and it is highly likely based on previous years that scammers will look to target them. Last year, HMRC issued a warning to students looking for jobs regarding potential scams. Scammers will use the HMRC brand to add credibility to their scams, such as phone calls relating to tax refunds or emails with links designed to capture personal and financial information.

As well as HMRC related scams, students may also be at risk of other scams, such as advertisements of fake jobs, particularly now with high numbers of vacancies for retail and restaurant staff, money mule recruitment and rental fraud. As mentioned earlier in the report, there has been a recent increase in the numbers of reports relating to direct debit refund scams, where individuals were recruited via social media, and this may be another area of risk for students. In addition, fraudulent investment related opportunities advertised through social media could also target students looking to make money. In the last MTU, there were reports of a new scam targeting students, whereby students were being approached or recruited whilst on public transport by suspects utilising the iPhone Air Drop messaging function. The concern is these individuals are being recruited as money mules or persuaded to invest in a non-existent scam.

The threat of fraud and cybercrime to students may be further exacerbated by current economic factors and the cost-of-living crisis.

Housing Scams

Recent homeowners are being warned about being cold called by scammers claiming that the recipient is entitled to a stamp duty refund. HMRC are warning that people could be targeted by tax repayment agents promising easy money but victims being left with a hefty bill to pay after agents have taken fees.

There has been a reported increase in the demand for rental properties as well as increased rental prices recently which is likely to continue due to several factors, such as the reduction in people purchasing property due to cost of living crisis. Rental related scams are predicted to rise because of the spike in prices and demand along with an increase in landlords exiting the rental market. This gap is particularly significant in city locations where competition for housing is fierce. These MOs are not new but current economic conditions could trigger increases in scams. Several sources have already started to see an uptick in reporting in relation to rental scams such as victims paying upfront for reasonably priced properties, without viewing, to avoid missing out.

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