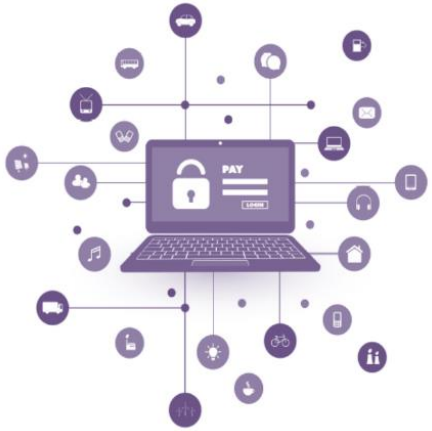
Monthly Threat Update - MTU Public– September 2022

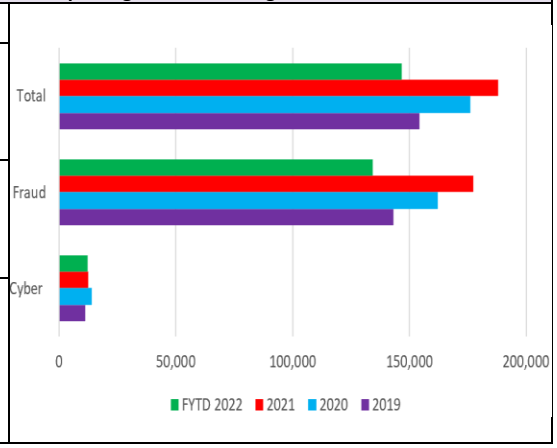
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1st -31st August 2022.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in August 2022		
	Report	Direction
Total	29,024 **0%**	↑
Fraud	26,876 **0%**	↑
Cyber	2,148 **5%**	↑



Explanation of Figures: The columns above on the left show the crime reports (excluding information reports) received for August 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 reports have remained consistent to last month's figures and have not shown any significant increase. Cybercrime reports to Action Fraud have increased in August by 5% to 2,148. Overall, reporting figures show little change to July's data.

- When looking at the financial year to date (April – August 2022) as shown in the graph, overall reporting figures are significantly below the same period in 2020 and 2021 (during covid restrictions), however, the reporting volumes are proving to be similar, if a little below, the figures seen during the same period in 2019. 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 2019 but are below the figures for the same period in 2020 and 2021. These comparisons to previous years will continue to be examined in subsequent MTU's.

- **Total losses** for crime reports, which have been verified, showed a significant increase in August, by 128%, from **£343.1 million** to **£782 million.** This is significantly above the previous year average of £207.6 million.

- **Online Shopping and Auction fraud** (crime and information reports) has increased by 8% this month, after steadily decreasing months prior. Figures have generally been going down since a high reporting level in January 2021 and remain lower than pre-pandemic levels. As we approach Christmas, and shopping habits change, this will be an area which is predicted to increase and will therefore continue to be monitored.

- **Ticket Fraud** has been steadily increasing since restrictions were eased and events have opened once more. August has seen another month of increase in figures, albeit smaller than last month's comparison, rising by 3% in August. Levels remain reasonably high and with many big events continuing to take place over the end of the summer months and then into the festival period, this will be one to continue monitoring.

- **Mandate Fraud:** Crime and information reporting has shown a small increase of 2% in August with 296 reports. Mandate fraud is 26% lower than the previous year average. Reporting remains lower than pre-pandemic.

Current Reporting Trends

June MO's

- **Royal Mail Delivery Scams:** Between 1st and 7th August, 1,058 reports were sent to recipients purporting to be from Royal Mail, linked to rescheduled deliveries. Offenders are sending fake emails claiming they were unable to deliver people's packages. They include a link leading to fraudulent websites, which recipients are asked to click on to reschedule their delivery. They are then asked to provide complete address details, which provides an opportunity for offenders to steal personal details and financial details. This might then result in money being stolen from the targeted victim's account.

- **E.ON Summer Payments:** Between 8th August and 23rd August, 206 reports were connected to "E.ON summer payments and refund" scams. This is a resurfaced phishing campaign designed to deceive recipients. A similar MO was identified in May 2022. Offenders are continuing to exploit the cost-of-living crisis using these scams as a hook capitalising on the public's potential vulnerabilities. The offenders are promising an £85 refund due to an overcharge, with the goal to steal the recipient's personal information and reveal their bank details. In some cases, the emails have malicious software attached, which can infect their devices with a virus. This can then be used for follow-up frauds and/or to facilitate identity fraud.

- **Ofgem Phishing Scam:** Fraudsters are impersonating Ofgem to target the public with energy rebate scams, during times of financial hardship. This type of scam has been reported, via the Suspicious Email Reporting service (SERs), to Action Fraud over 1,500 times already in two weeks, between 5th August – 22nd August. The malicious emails provide links to the recipient to apply for the rebate and/or refund. Once the victim has entered their details, criminal use this to steal their personal and financial information for their own gain. All reported emails contain the email subject header "Claim your bill rebate now". Fraudsters try to make the communications appear authentic by using Ofgem logos and colours.

Horizon Scanning – Monitoring

New Cost of Living Scams: Fraudsters have consistently managed to adapt their tactics in line with societal changes and/or major world events. The looming recession as provided a particularly fertile environment for criminals to thrive in. A warning has been issued about new cost of living scams. Fraudsters are using multiple platforms to reach people of all ages, including email, telephone, and social media. As energy prices continue to rise and many are struggling to 'tighten their belts' any further, criminals are preying on vulnerable businesses and households by offering fake discounts on prepayment meters as well as hoax rebates schemes. Concerns have also been raised over doorstop scammers posing as tradesmen.

The Student Loans Company Urge Students to Remain Vigilant: As the new academic year begins, the Student Loan Company (SLC), has issued a warning reminding people to remain vigilant of student targeted scams. Scammers may send bulk emails/SMS messages around the time of when students are expecting a payment. They may include phrases which convey a sense of urgency such a 'failure to respond in 24 hours will result in your account being closed'. In addition, with many young people using social media, criminals have adapted to targeting victims through social posts and direct message on digital platforms.

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