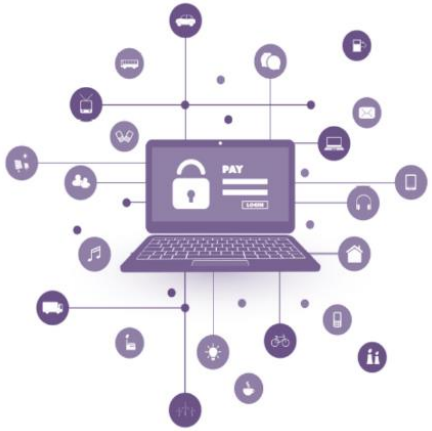
Monthly Threat Update - MTU

Public– August 2022

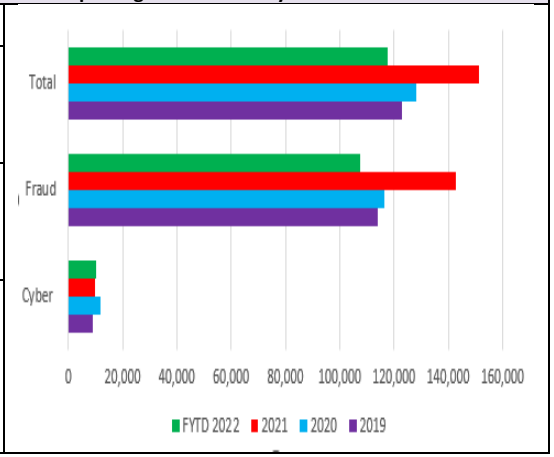
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1st -31st July 2022.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in July 2022		
	Reports	Direction
Total	28,903 **1%**	↑
Fraud	26,852 **3%**	↑
Cyber	2,051 **-18%**	↓



Explanation of Figures: The columns above on the left show the crime reports (excluding information reports) received for July 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 increase in July by 1% to 28,903.

- When looking at the financial year to date (April – July 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 proving to be similar, if a little below, the figures seen 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 2019 and 2021 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, increased in July, by £67.8million, from **£249.7 million to £343.1 million.** This is significantly above the previous year average of £207.6 million.

- **Lender Loan fraud** (crime and information reports) have stayed consistent and overall levels remain at the highest number of reports since March 2021. This fraud is predicted to continue to rise due to the cost-of-living crisis, so this is one to monitor over the coming months.

- **Ticket Fraud** has been steadily increasing since restrictions were eased and events have opened once more. July has seen an increase in figures, by 23% in comparison to June. Levels remain reasonably high and with many big events continuing to take place over the summer months and then into the festival period, this will be one to continue monitoring.

- There has been an increase in reports under the category NFIB3G, which relates to Retail Fraud. Figures have risen by 18% this month, however, it remains below the 2021-year average.

- Other Financial Investment reporting has increased in July by 4%. Reporting is now 10% above the previous year average. Shares Sales have decreased by 2%. Pyramid and Ponzi schemes have decreased this month by 31%, following an increase in reporting from the previous month (June), reporting is now up 26% from last year average. Pyramid and Ponzi and Other Investment are higher than pre-pandemic.

Current Reporting Trends

June MO's

- **EVRI Scams:** A high number of reports (majority are info only) are being received in relation to a new phishing text message purporting to be from EVRI stating 'your parcel has a £2.99 unpaid shipping fee, pay this now at *link provided*. Failure will result in your parcel being returned to its sender'. Victims are then providing personal information and bank details via this fake link.

- **Fake Emirate Holiday Giveaways:** A new scam alert has been issued, warning people of fake Emirate holiday giveaways. The offer invites potential victims to click on a link to be in with a chance of winning one of the 5,000 free round-trip holidays. The scam is being run through WhatsApp and has also appeared on Facebook. Google searches for 'Emirates ticket giveaway' have risen by 4,050% in the first week of August alone[1].

- **Ticket Scams (Football):** Football fans are falling foul of ticket scams on social media sites, such as Twitter and Instagram. With the new season of football beginning, supporters are being warned of a potential rise in ticket scams.

- **UPS Delivery Scams:** NFIB warn of UPS delivery scams. 1,697 reports were made regarding contact made from the 'UPS Customer Support Team'. Offenders are sending fake emails claiming that they were unable to deliver packages as there was no one in. Emails include a subject heading of "Outstanding Delivery (ID#34632900-371?)". Recipients of the email are asked to click on a link to a fraudulent website to reschedule delivery. This allows fraudsters to collect personal and financial information on the victim. Emails include playback videos, hyperlinks and even brand logos in an attempt to look authentic.

- **Amazon Gift Card Scam:** Emails are being sent to potential victims, purporting to be from Amazon. The scam offers recipients the chance to win an Amazon Gift Card worth £1,000. The emails are given the subject header "We have a surprise for you! £1000 Amazon Reward" with a URL link provided in the main body of text. These emails also attempt to replicate a genuine email from Amazon and look authentic and convincing especially as they contain hyperlinks and brand logos. The scam is used to collect and steal personal information, which can then be used for PII and credential harvesting, for follow-up frauds or/and facilitation of identity fraud.

Horizon Scanning – Monitoring

Friend in Need:

A new 'friend in need' scam is targeting Whatsapp users. Criminals are posing as friends or family members[2] in need of help. They will text from what they claim to be a new mobile after their old one was 'lost/damaged'. They will then go on to ask for money to pay an urgent bill/new phone. Recent scams have even initially asked for funds to be transferred to a friend or family member before being sent on to the scammer to give the appearance of an initial low risk payment[3]. Losses are totalling over £1.5 million already. Northamptonshire police have issued a warning to

[1] Scam alert: watch out for this fake Emirates holiday WhatsApp giveaway - Which? News

[2] 'Friend in need' scams costs Whatsapp users £1.5 million | Action Fraud

[3] Fraud expert warns of twist to fake 'Hi mum, hi dad' messages (yahoo.com)

Whatsapp users in Northamptonshire after 14 users lost £24k in May and June alone. This mode of operating is also referred to as the "Hello Mum" or "Hello Dad" scam. Losses may continue to increase as students head off to university in September, giving criminals further opportunities to exploit family members and friends.

New Omicron Jab:
There is to be a new Omicron Covid vaccine to be rolled out within the next few weeks, as the UK become the first country to approve the specifically tailored jab, ahead of fears for winter spikes. With the rollout for the latest booster, there are concerns that covid related fraud may increase as a result, with criminals targeting potential victims with vaccine scams, not too dissimilar to the ones seen previously. This will be an area which will continue to be monitored.[4]

Energy Price Cap:
With with the severe increase in the energy price cap reported last week, fraudsters are likely to seize this opportunity to exploit those looking to change energy provides and/or tariffs. Individuals are being warned to be vigilant to avoid falling victim to new 'ishing' campaigns associated with energy supplies, for examples offers which seem too good to be true or fake rebates.

'Check-a-Website':
Get Safe Online have partnered with Cifas to launch '**Check-a-Website'** which is a new feature hosted on the Get Safe Online website which invites users to check if a website is safe before accessing it. The service uses an algorithm which provides a trust score based on more than 40 data sources as well as thousands of malicious websites from law enforcement, regulators and brands each week.

CyberAlarm Tool:
An enhanced version of Police CyberAlarm tool has launch which assists individuals and businesses to block malicious ransomware and identify weak spots in computer systems. The data collated is then used to create reports where vulnerabilities can be identified and assist users in better protecting themselves. Police forces across England and Wales are also using this tool to help develop their understanding of the threat to the public and the changing landscape of cybercrime. The latest version of the CyberAlarm tool has new capabilities in anti-spam, anti-virus and intrusion protection/detection systems[5].

Cost of Living Crisis Scams:
With the cost of living crisis deepening scammers will be using the economic downturn to their own benefit. The warning comes as many are due to receive a first instalment of a cost of living payment, worth £326. Reports have been received of fraudsters attempting to exploit vulnerable people with the promise of money saving schemes, including, energy and council tax rebates or phishing exercises encouraging individuals to apply/claim a 'cost of living payment' via text, followed by an email to gain further information from the victim.

[4] New Omicron jab to be rolled out within weeks after UK becomes first country to approve it (inews.co.uk)
[5] Enhanced version of Police CyberAlarm tool launched | UK Police News - Police Oracle https://www.policeprofessional.com/news/police-cyberalarm-monitoring-tool-goes-live-with-major-upgrade/

Student Related Fraud:
Student related fraud, as discussed in previous updates, continues to be an ongoing threat over the coming months with fraudsters targeting many people heading off to university this year. Cases include scammers sending fake emails asking for student fees to be paid in advance.

Students continue to be at risk of other scams, such as money mule recruitment, rental fraud and advertisements of fake jobs, particularly now with high numbers of vacancies for retail and restaurant staff. The threat of fraud and cybercrime to students may be further exacerbated by current economic factors and the cost-of-living crisis.

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