Monthly Threat Update - MTU
Public– September 2021

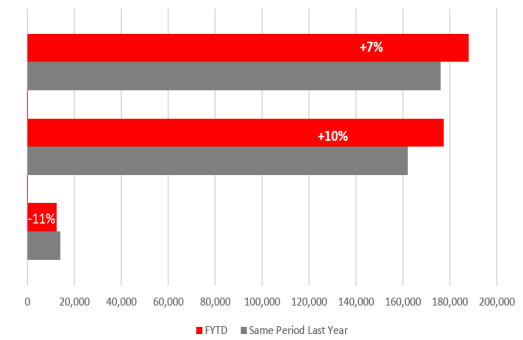
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends.

Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in August 2021

	Reports	Direction
Total	36,977 **+1%**	↑
Fraud	34,407 **+1%**	↑
Cyber	2,570 **-2%**	↓



- **Crime reports** have increased slightly in August; however, reporting (including both crime and information reports) has **decreased** from 51,661 to 49,680.

- **The following continuing threats have been observed consistently over the past few months; Lottery Scams** continue to rise each month; **Rental fraud** has had another increase in reports and **Ticket Fraud** has jumped again in August with reporting now at the highest level since November 2019.

- **The following emerging threats have been observed from August 2021 data; Online Shopping & Auction Fraud** reporting has significantly increased this month compared to the previous month but is still lower compared to previous lockdown months. It is predicted that this fraud type will start to increase in the run up to Christmas and afterwards. Reports relating to **Abuse Of Position of Trust** have jumped this month and are now at the highest levels since reporting began. **Fraud Recovery** reports have increased in August, the highest number of reports for this fraud type to date.

- After a drop in reporting in June, **Dating Fraud** reporting has significantly increased in August. This is the highest volume received in one month for this fraud code to date. This increase in reporting is likely due to online dating websites predicting an influx of increased signups over the summer, which was raised in a previous MTU. **Share Sales** has increased slightly from last month but still shows a drop in reporting compared to between February and May 2021. **Other Financial Investments** reports have continued to increase and are now at the highest reporting levels since the MTU began. **Mandate Fraud** has jumped up after a drop last month and is now at the highest volume reported in a month since March 2021. **Cheque, Plastic Card and Online Bank Accounts** continues to drop in reporting and is the lowest amount since MTU reporting began. **Hacking – Social Media** reports has been increasing steadily over the past few months to the highest volume since June 2020.

Current Reporting Trends

August MO's

- Websites purporting to offer driving licence renewals featured frequently once again, whilst reports relating to car auction purchases, garden furniture, gaming consoles, white goods and designer clothes from various websites which were never received. Numerous reports were also received relating to cryptocurrency investment schemes in various platforms where victims haven't seen any returns on their investments. Finally, several victims have reported booking golf holidays this month, through a website and then finding out the booking hadn't been made, even though money had been taken.

- Action Fraud received numerous reports within 48 hours relating to fake emails purporting to be from Asda. The emails stated that the recipient can win a £100 promo reward gift card' by completing a marketing survey. The links provided in the emails lead to phishing websites that are designed to steal personal information.

- Banking branded phishing messages continue to be reported with the most common being registering for a new device or new payment details being set up with the recipient encourage to click on the link to set up or cancel a payment. Two new MO's informs the recipient of the message that they have successfully amended their number and to click on the link if they did not make this change and the other relates to the alleged creation of a large direct debit payment.

- Reports were received in August relating to a company offering PCR tests to travellers returning from holidays. The tests were ordered and paid for but were never received.

Horizon Scanning – Emerging Issues & Threats

Covid Related Scams

Any potential increases in Covid and pressure on the NHS as well as any possible introductions of new restrictions could lead to the reintroduction of many of the MO's used by fraudsters and cyber criminals during the previous lockdowns and restrictions.

JCVI have recently announced that those over 60 as well as those with severely weakened immune system will be invited to have a third vaccine as well as the offer of a vaccination for 12- to 15-year-olds. Any further vaccine rollouts may be exploited by scammers contacting those eligible to gain personal and financial information from them.

Over recent months, cross-sector agencies have detected a significant increase in scams relating to the COVID Pass to steal money, financial details, and personal information.

So What?: The reintroduction of Covid MO's devised by fraudsters in order to trick victims into handing over personal and financial details following further restrictions, vaccine passports or the rollout of booster jabs.

Provenance: Anti-vaxxers offered fake NHS Covid-19 passes and vaccine cards on Telegram (msn.com)

COVID-19: Vaccine passports will be introduced at big venues to avoid winter closures, minister says | Politics News | Sky News

Health and Social Care Reforms

The Prime Minister made a statement at a press conference on health and social care that they will be setting the limit to what elderly people will have to pay for their care, regardless of assets or income. In England, from October 2023, no-one starting care will pay more than £86,000 over their lifetime. Nobody with assets of less than £20,000 will have to pay anything at all, and anyone with assets between £20,000 and £100,000 will be eligible for means-tested support.

So What?: As a result, could pensioners have more assets and available funds because of this change, and could this make them at increased risk of being targeted with various frauds and scams in the future?

Provenance: Social care funding reforms announced in England – Which? News

Scams Targeting Students and Young People

A recent study found that the fastest growth in fraud is amongst those under the age of 21. Although based on US data, we are likely to see similar findings in the UK. The study finds that this age group is more comfortable to being online and sharing personal information, which makes them more susceptible and trusting to falling for a scam.

HMRC have issued a warning to students looking for jobs regarding potential scams. With higher numbers attending university, it is likely many will be looking for jobs to support their studies. 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.

So What?: Students and young people may be particularly vulnerable to scams. Fraudsters and cyber criminals may try to exploit in several ways.

Provenance: HMRC warns students of scams | HM Revenue & Customs (HMRC) (mynewsdesk.com)

Teens falling prey to online scams faster than their grandparents (cnbc.com)

Record number of first-time buyers used Help to Buy last year | This is Money

https://www.cypnow.co.uk/news/article/young-people-to-be-hit-hardest-by-end-of-universal-credit-uplift

Deep Fakes

DeepFakes have already been highlighted as an emerging threat in previous MTU's but recently there has been concern around the increasing current risk that deepfakes pose to fraud and cybercrime. In March, it was reported that the FBI stated that it expected fraudsters to leverage 'synthetic content for cyber….operations in the next 12-18 months'. Although relatively new, there are already reported instances worldwide of cybercriminals using AI to target victims. Business security teams have already reported deepfakes being used in phishing attempts and Business Email Compromise Scams.

So What?: AI presents a significant cyber and fraud threat to the UK and we are highly likely to see increases in cyber and fraud reports with AI as an enabler in the near future; for example, sextortion scams, dating scams and investment frauds, however, we could see AI being used to enable many other cyber and fraud types.

Provenance: Scammers are using deepfake videos now. (slate.com) Deepfakes in cyberattacks aren't coming. They're already here. | VentureBeat

Distribution List

Organisation	Department / Role	Name
PUBLIC		

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018.

The cover sheets must not be detached from the report to which they refer.

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