

Monthly Threat Update - MTU

Public– January 2021

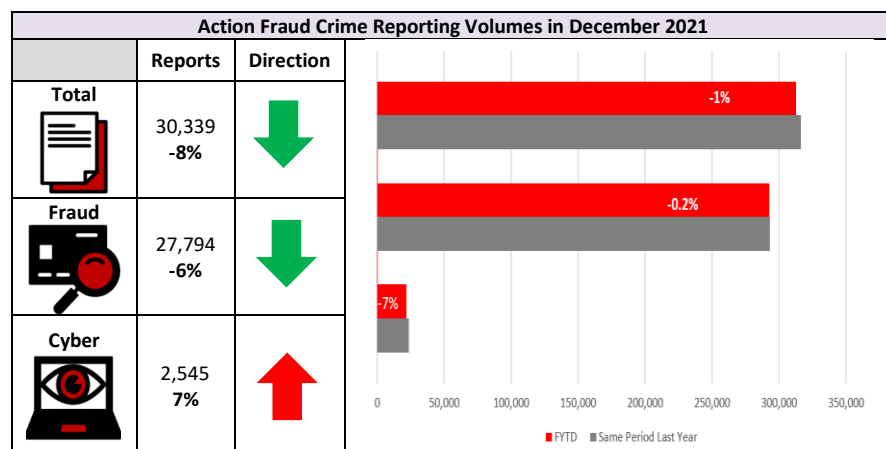
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends.



Contents:

- [Crime Trends Summary](#)
- [Current Reporting Trends](#)
- [Horizon Scanning – Emerging Issues & Threats](#)
- [Distribution List](#)

Crime Trends Summary



- **Both Crime and information reports for fraud** have slightly decreased in November from 44,852 to 42,760. This is still lower than the baseline average for fraud and cyber reporting but follows similar reporting levels pre-pandemic. For both crime and information reports, 16 out of 54 fraud types showed an increase in reporting compared to the previous month, whilst 26 out of 54 fraud types showed an increase in reporting compared to the same time last year.
- Whilst fraud reporting has dropped in December, cyber-crime reporting has increased by 7%. Hacking – social media has increased again, though not as rapidly as the previous month but is still higher than the year-to-date average. Hacking – Personal has increased 11% after a continued drop in reporting since July 2021 and is higher than the year-to-date average. Hacking – Server has also increased. Hacking – Extortion also shows an increase of 15% but remains below the year-to-date average.

- **Advance Fee Fraud reports** have increased once more after a drop in reporting in November. Reporting has been gradually increasing over the past few months after a rapid drop in reporting from the highest level in April 2021. **Other Advance Fee Fraud** reporting follows a similar pattern and has increased for the second month in a row after seeing a drop in reporting since the highest level in March 2021. This increase mirrors the increase in Authorised Push Payment frauds that banks are seeing being reported now. In addition, it is reported that this increase coincides with a significant increase in people looking for short term loans.
- Crime reporting mentioning **Covid-19** has increased to 520 after a drop in reporting to 313 reports in November. This is now above the baseline average of 500 and is likely to be due to the introduction of Plan B measures in response to the Omicron variant. There was an increase in the number of reports received in relation to COVID Passes/Passports/Certificates/Documents in December. In the week commencing 13/12/2021 we saw an increase in COVID Pass reporting which is in line with the recent policy update where it is now required to show an NHS COVID Pass to enter certain venues and events.
- **Computer Virus and Malware Fraud:** Reporting has risen by 6% but still 22% below the average for the year and 24% below the previous year.

Current Reporting Trends

October MO's

- Covid themed scams continue to be received. Reports were received in December in relation to a company purporting to offer day 2 PCR testing. The tests were never received, and the customers have been unable to contact the company. We've also started to see reports (since the beginning of Jan) where victims are receiving text messages stating they have been in contact with someone with Omicron and that they need to order a PCR test. The victim follows a link to a website where personal and banking information are requested.
- There have been a few reports received about a disturbing hacking whereby the suspect takes over a social media account and they have then uploaded explicit images of children in a thumbnail and then demanded money for the victim.
- Numerous reports were received last month in relation to correspondence being sent from a legal company purporting to be collecting outstanding payments for an energy company.
- A significant number of reports are still being received in relation to ticket fraud, following the cancellation of a North Pole experience where the organisers have ceased contact. In addition, reports are continuing to be sent to Action Fraud about an online company purporting to sell football kits online; the victim places an order and pays for the goods, but the items are never sent.

So What?: New MO's devised by fraudsters in order to trick victims into handing over personal and financial details.

Provenance: SAIP data

Horizon Scanning – Emerging Issues & Threats

Holiday Related Fraud

The introduction of Plan B measures towards the end of 2021 led to a decline in holiday and flight bookings due to the PCR requirements when returning from the holiday destination.

However, this week it has been announced by the government that they were scrapping PCR testing rules, so now fully vaccinated people returning to the UK will no longer need to take a Covid test before travelling and will not need to self-isolate until they receive a negative test result after arrival. The relaxation of these rules in the past week has led to have a significant surge in holiday bookings being reported by airlines and holiday companies. In addition, France's easing of restrictions for UK travellers has led to an increase in bookings for ski holidays.

There have also been reports of an increase in prices following the rule easing. It is likely that the demand for overseas holidays and increases in price will lead to consumers searching around for the best deals, this is likely to be exploited by scammers. The most popular destinations reported are Spain, Greece, France, Italy, US and Portugal and it likely we will see ticket or accommodation fraud reports relating to these destinations.

In addition, the ongoing requirement to produce Covid-19 vaccination records as a condition of travel has increased the risk of falsification of

vaccination records by insiders for financial gain. Scammers are also continuing to offer false vaccine records for sale on social media. Some UK forces are already investigating some cases of altered vaccination records and the same is being reported elsewhere in Europe. It is likely this risk will continue to increase following the surge in holiday bookings, with non-vaccinated people looking to travel abroad.

So What?: These change in rules are likely to be exploited by scammers as people look to book holidays abroad this year.

Provenance: [Top holiday destinations revealed as half of people 'already planning' overseas trips next year | Travel News | Sky News](#)

[French holiday bookings surge after rule change - BBC News](#)

[Jet2 reports bookings rush with holiday sales up 150% since travel rule changes - Cheshire Live \(cheshire-live.co.uk\)](#)

[Covid travel news: Will you book a holiday as prices 'skyrocket' - restrictions axed? | UK | News | Express.co.uk](#)

[Relaxed Covid travel rules spark holiday BOOM \(msn.com\)](#)

[French holiday bookings surge after rule change - BBC News](#)

<https://www.wantedinrome.com/news/italy-police-bust-fake-covid-vaccine-scam.html>

Rising Living Costs

There has been a lot of news reports about the increasing living costs and family budgets coming under pressure over the coming months, with price rises due to soaring inflation, rising energy costs, increased train prices, increased interest rates and taxes. In addition, some businesses are set to raise prices due to rises in raw material costs, Brexit, and the impact of the pandemic. There have already been reports of struggling households dipping into savings to fund the increasing cost of living. As mentioned previously in this report concerns have been raised about the reliance on BNPL schemes, with the risk that many people will not be able to make the repayments and could increase the numbers of people in debt.

Retired people are predicted to face a tricky year as the state pension will only rise by around 3%. Savings rates are still very low, and mortgages are set to become more expensive for homeowners, particularly young people trying to get onto the property ladder.

As millions of people face hardship due to rising contributions and tax burdens this is likely to have a knock-on effect making them vulnerable to becoming a victim of fraud or falling into crime themselves.

Examples of such scams include increases in cryptocurrency scams as people look to invest outside of traditional savings accounts, online shopping fraud as consumers search for better prices and advance fee frauds, where people try to take out loans to help with rising costs. Fraudsters are likely to exploit the concerns around gas prices in various ways, e.g. doorstepping offering scam deals, cold calls around new gas takeovers or phishing emails and texts relating to updating personal and financial information.

So What?: Rising living costs are likely to have both a direct and indirect impact on the fraud landscape.

Provenance: <https://www.thisismoney.co.uk/money/article-10375213/Three-five-firms-set-hike-prices-coming-months.html>

[Ex-HSBC boss's stark warning around young people and property debt | This is Money](#)

[Why gas and electricity prices are rising – and how to protect yourself \(telegraph.co.uk\)](#)

[Millions worse off as low-income families face “real pain” due to Budget taxes, IFS warns \(inews.co.uk\)](#)

[One in four who celebrate Christmas will struggle to afford it - Your Money](#)

<https://www.google.co.uk/amp/s/inews.co.uk/news/politics/rail-fare-increase-train-prices-rise-march-2022-uk-edited-1357309/amp>

[Struggling households dip into savings to fund soaring cost of living | UK News | Sky News](#)

[Interest rates rise for first time in three years - BBC News](#)

[Beat the cost of living crunch: Key dates for your financial calendar | This is Money](#)

[What you need to know about pensions in 2022 | This is Money](#)

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

Copyright © City of London Police 2021 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this Alert, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this Alert, please contact the City of London Police. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.