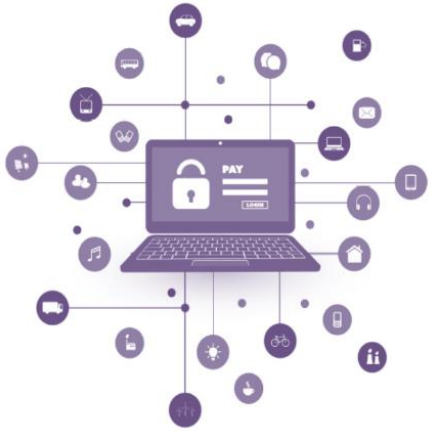
Monthly Threat Update - MTU

Public– December 2021

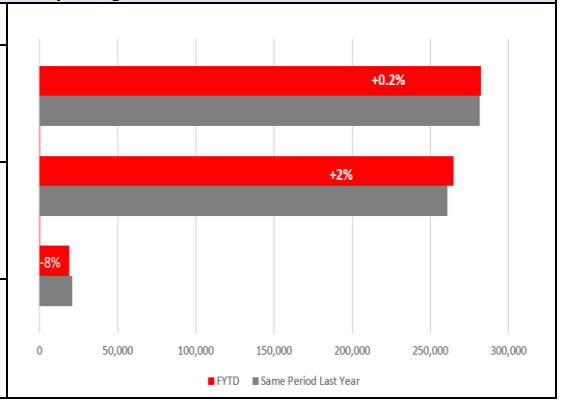
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in November 2021		
	Reports	Direction
Total	31,787 **-4%**	↓
Fraud	29,401 **-5%**	↓
Cyber	2,386 **9%**	↑



- **Both Crime and information reports for fraud** have slightly decreased in November from 45,656 to 44,852. However, 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, 29 out of 54 fraud types showed an increase in reporting compared to the previous month, whilst 23 out of 54 fraud types showed an increase in reporting compared to the same time last year.

- The increase in reporting for Cyber-crime is mainly due to a 24% increase in Hacking – Social Media reporting which is the highest volume for this fraud type since June 2020.

- **Other Advance Fee Fraud** reports have increased for the second month in a row after seeing a drop in reporting since July. Reporting is still below the year average. **Online Shopping and Auction** fraud has begun increasing again after a drop in reporting over the past few months. We would expect reporting to continue to increase.

- **The following emerging threats have been observed from November 2021 data; Pyramid/Ponzi schemes (increase of 44%), Other Consumer Retail Fraud (increase of 13%), Hacking – social media (increase of 24%), Application Fraud (increase of 6%) and Telecom Industry Fraud (increase of 25%)** all show increases from the previous month, and all apart from online shopping remain higher than the overall baseline average for the fraud type. Telecom Industry Fraud shows the highest level of reporting since February 2019.

- **Investment Fraud** reporting has risen again after a slight drop in reporting over the previous two months and is higher than the baseline average. A large proportion of these reports relate to individuals being contacted through social media or instant messaging and persuaded to invest. These relate to reported increases in younger people investing and people looking to invest outside the mainstream banking system currently offering low interest rates.

- **Courier Fraud** crime reports increased significantly from 179 to 364. Reporting is higher than YTD and previous year's average. This is the highest reporting since March this year. A high percentage of these reports relate to calls purporting to be from the police claiming fraud had taken place on the victim's card.

Current Reporting Trends

October MO's

- Online fraudsters have quickly reacted to news of the new COVID-19 variant Omicron, with a carefully crafted phishing campaign. These new phishing emails are designed to appear as if they are sent from the NHS and urge recipients to get an 'Omicron PCR test' for the new variant. The bogus emails falsely claim that the new variant requires a new test kit. They feature a link, legitimate looking 'get it now' button and are sent from 'NHS Customer Service'. The emails also invite readers to visit the site shown in the image below. However, clicking the link takes you to a phishing site, which then asks users to enter their full name, date of birth, address, mobile number, email address and their mother's maiden name – which scammers could use to craft follow-on identity fraud attacks. It also asks for a payment of £1.24 for 'delivery'. Presumably, if users proceed with this, they will also have their bank card details stolen.

- Action Fraud have issued an alert to warn people about fake emails claiming to be from Martin Lewis after receiving 300 reports in one week[1]. The message from the well-known financial advisor on social media is entitled 'Martin Lewis: we are in crisis. Follow this revolutionary way to survive financially'. The links in the emails lead to phishing websites that are designed to steal your personal and financial information. Martin and other public figures have written to the PM to request that scam ads are included in the Online Safety Bill[2].

- Members of the public in Milton Keynes are being warned about a delivery fraud targeting people selling goods on online marketplaces[3]. The victim is contacted by the scammer saying that they wish to buy the item, often a bulky item like furniture, and a Fedex delivery person will collect the item and a money order will be made through the delivery company to pay for the goods. The victim selling the item is told that they need to pay a £50 insurance fee which will be reimbursed by downloading a special coupon. The scammers direct the seller to the Dundle payment site, to purchase a gift card, instructing the seller to email them the code once purchased.

- Police Scotland have been warning members of the public about rental scams[4]. In one scam, the person showing the viewers around the rental property was unknowingly recruited by the fraudster whilst looking for a job online. The individual then showed people around a property they believed was for rent, the potential renters paid a deposit to the suspect who then ceased all communication.

- **Advance Fee Fraud MO's –** Last month Action Fraud reported on the MO where WhatsApp messages are sent to parents purporting to be from their child. The message states that the child has changed mobile numbers and then requests some money from the parent, giving a variety of reasons why. The scam seems to have continue, with people reporting that that they are now receiving messages purporting to come from the parent.

[1] Martin Lewis scam: Action Fraud issues urgent warning | This Is Local London
[2] Martin Lewis, Sir Richard Branson, Deborah Meaden and other public figures issue plea to the PM to put scam ads in the Online Safety Bill (moneysavingexpert.com)
[3] Warning: Scammers launch 'FedEx' fraud on unsuspecting victims in Milton Keynes | Milton Keynes Citizen
[4] The students losing thousands in an Edinburgh rental scam - BBC News

Horizon Scanning – Emerging Issues & Threats

Covid Related Scams

As mentioned earlier in this report, we would expect fraud reports with the Omicron variant being used as a hook to continue to be reported. We would also expect fraud reports relating to Covid Passes to continue to be received over the coming months, particularly as fraudsters look to take advantage of people booking holidays for next year. We may also see an increase in scams in relation to booster injections; booster invitations have been brought forward and opened up to over 18's to increase take-up before winter. Any confusion around the new variant and new PCR testing rules is likely to be exploited by scammers.

The implementation of Plan B measures due to the new variant could also lead to an increase in demand for counterfeit certifications or other fraud reports relating to Covid passes. In addition, any measures around working from home could lead to an indirect impact on the fraud landscape and could increase fraud and cyber volumes once more. Online shopping is likely to increase in the lead up to Christmas and it is suggested an increased number are likely to prefer buying gifts online to on the high street; this threat is further increased by more people working from home and therefore likely ordering online as a result.

So What?: These announcements are likely to have both a direct and indirect impact on the fraud landscape.

Provenance: All adults to be offered COVID-19 boosters by end of January - GOV.UK (www.gov.uk)
JCVI advice on COVID-19 booster vaccines for those aged 18 to 39 and a second dose for ages 12 to 15 - GOV.UK (www.gov.uk)

https://www.yourmoney.com/household-bills/one-in-five-brits-hoping-to-avoid-high-street-shopping-this-christmas/

Boosters to be added to NHS COVID Pass for travel - GOV.UK (www.gov.uk)

Criminals with 'advanced forging capabilities' selling valid vaccine certificates on dark web | Science & Tech News | Sky News

Do not fall for this PCR scam that can't even spell Omicron | Metro News

So What?: Seasonal trends are likely to have an impact on fraud and cyber reporting.

Spiking Reports linked to Fraud

There has been a lot of media coverage nationally around a reported increase in females being spiked or injected. In addition, there has been some further reporting around people being spiked and then having their bank or other accounts compromised where a significant amount of money is then taken. Twenty-nine Action Fraud reports that mentioned 'spiking' or being 'spiked' were received between September and mid-December. All victims believed that they were spiked prior to debit cards and Sim cards being stolen and then money being transferred out of their bank accounts. Some victims recall being escorted to a cash point. Other victims report that their PayPal was also hacked, and cryptocurrency purchased. All these incidents took place at licensed premises or at house parties.

So What?: In response to the national increase in drink and injection spiking incidents, we need to understand the scale of the incidents linked to fraud in order to develop recommendations around Prepare, Protect, Prevent and Pursue.

Provenance: Action Fraud

Festive Scams

Previous MTU's have discussed some of the scams predicted in the run up to Christmas. As mentioned, some of these scams such as online shopping and auction fraud may increase further with the new Covid measures that have been brought in. Even prior to the Plan B measures, a survey suggested that a fifth of those interviewed were intending on shopping online this Christmas, rather than on the high-street. Warnings about fake reviews have also been raised to those buying online.

As well as online shopping and auction fraud, people are being warned about online loan fraud in the run up to Christmas, with individuals searching for loans online when they have been turned down by their bank.

So What?: MO's designed to target unsuspecting people online in the run up to Christmas.

Provenance: One in five Brits hoping to avoid high street shopping this Christmas - Your Money

Vulnerable people targeted by online loan fraud ahead of Christmas (irishexaminer.com)

Festive Shopping Period Is When Shoppers Are Most Vulnerable to Cybercrime | The Fintech Times

Christmas shoppers warned about fake online reviews - here's how to protect yourself | Business News | Sky News

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