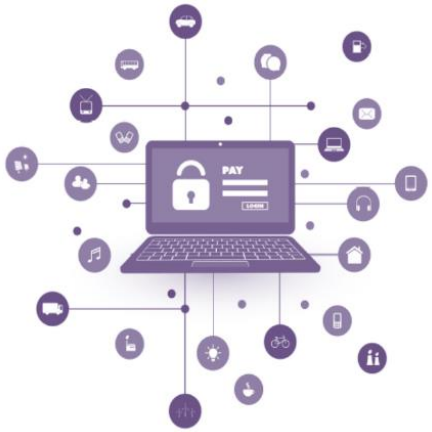
Monthly Threat Update - MTU Public– March 2022

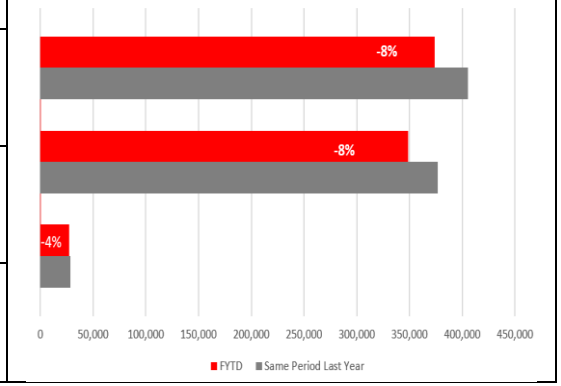
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1st February – 28th February 2022.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in February 2022		
	Reports	Direction
Total	30,810 **0.3%**	↑
Fraud	28,191 **1%**	↑
Cyber	2,619 **-4%**	↓



- **Both Crime and information reports for fraud** have slightly decreased in February by 1% to 44,087. This is lower than the same time last year. For both crime and information reports, 34 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.

- **Cyber-crime reporting** has fallen in February by 4%. Although reporting has fallen slightly last month, crime reports remain higher than throughout most of 2021. **Hacking – Extortion** continues to show a rise in reporting with reports approaching pre-pandemic levels once more.

- **Fraud Recovery** reporting has increased slightly and is now at the highest reporting since November 2021. Figures remain higher than pre-pandemic.

- Reports relating to **Rental Fraud** continue to increase after a drop in reports towards last year. This increase was discussed in the last Monthly Threat Update.

- As reported last month, we continue to see an increase in Investment type fraud reports. **Pyramid and Ponzi schemes** have had a significant jump in reporting in February and reporting is now at the highest level since reporting started. **Other Financial Investments** also show reporting at the highest level. **Share Sales Fraud** figures were decreasing in reporting after a peak in March 2021, but figures have jumped in February to the highest since May 2021.

Current Reporting Trends

January MO's

- People have been receiving text messages informing them that they have been in close contact with someone with Omnicron and that they need to order a test. The text message provides a link which requests their personal details as well as banking information to pay a couple of pounds for the tests to be sent out.

- Reports have been received in February in relation to individuals selling their old mobile phones in exchange for cash. The phones are sent to the company, but money isn't never paid out to the sellers. Any correspondence sent to the company is then ignored.

- Action Fraud have issued an alert in relation to emails purporting to be from Tesco. 197 reports were received in one week regarding an email that claimed that customers could win free shopping by entering a

competition. The links in the emails directed recipients to a phishing website designed to steal personal and financial information.

- Scammers continue to use concerns over energy prices to target victims. Reports relating to calls and emails purporting to be from utility companies continue to be received. As the price cap increases on 1st April, we would expect to see a significant increase in these reports.

- A warning has been issued in relation to a fake Royal Mail scam that is currently in circulation. The scam targets victims using a fake chat bot to discuss a missed payment which then is used to sign up victims to expensive subscriptions[1].

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

Provenance: SAIP data

[1] Warning over Royal Mail chatbox scam that signs you up to subscription - Wales Online

Horizon Scanning – Emerging Issues & Threats

NFT's

Non-Fungible Tokens (NFT's) is a unit of data stored on a blockchain that can be sold or traded. Tokens can represent ownership of unique items, such as art or other collectibles. Non-fungible means that it is unable to be traded for the same thing, it is one of a kind. NFT's have increased in popularity over the past year alongside the rise in cryptocurrencies. Celebrities, such as David Beckham, received announced involvement in NFT's and the Treasury have just requested for the Royal Mint to create a non-fungible token by the summer[2], pushing the tokens into the mainstream.

Along with the rise in popularity there has been criminals looking to exploit this area. The market currently lacks regulation and due diligence which leaves it open to abuse. According to Chainanalysis, one MO involves 'wash trading' whereby the criminal is involved in both the seller and buyer side and sells the token for a higher price to a wallet that they also own. In addition, money launderers have been able to take advantage of this digital asset realm, alongside other criminals in crime areas such as drugs and terrorism looking to transfer criminal funds. Other popular scams include scammers selling NFT's that don't exist, or they don't own. There have been other reports of NFT's being stolen through phishing scams due to weaknesses in the system and scams prioritising a scammer's NFT and wallet over other sellers' tokens.

It is likely the increase in the popularity of NFT's will lead to a rise in volume and range of MO's around NFT fraud.

So What? As people continue to invest in NFT's, it is likely frauds relating to this area will increase.

Provenance:

David Beckham to launch his own NFTs (proactiveinvestors.co.uk)

Are NFTs Turning Into a Hotbed for Crime? (fool.com)

A handful of NFT users are making big money off of a stealth scam. Here's how 'wash trading' works | Fortune

New tech, old scams: Don't fall for these crypto and NFT ripoffs - CBS News

Rishi Sunak asks Royal Mint to create NFT | Non-fungible tokens (NFTs) | The Guardian

Cent Stops Selling Most NFTs Due to Fraud | PYMNTS.com

UK Law Agents Seize NFTs | Global Finance Magazine (gfmag.com)

Attackers phish $1.7 million in NFTs (computing.co.uk)

NFTs: New Fraud Targets (forbes.com)

Russian Invasion of Ukraine

The NFIB have received reports relating to fraudulent charity donations and appeals to support Ukraine. Some of these reports request donations to be made through bitcoin or other cryptocurrencies. The crisis is also being used by investment fraud scammers as a reason not to pay out. Phishing emails are being received by Microsoft users claiming that there has been unusual sign in activities from a user in Russia. The link contained in the email is designed to steal personal and financial information. Calls are also being received purporting to be from the recipient's bank fraud department advising that several payments have been made to Russia.

Boris Johnson has brought forward the Economic Crime Bill to produce a new public register for UK property owners. It's estimated that £170bn worth of UK property is held by anonymous owners overseas hiding behind shell companies. It allows these owners, including Russian oligarchs to avoid publicity, tax or worse. The register will force the identity of the ultimate owner to prevent foreign owners from laundering their money in UK property. It will provide transparency, and if owners do not comply with this, owners may have selling restrictions applied to their property and potentially receive a 5-year sentence.

Many want to help Ukraine, but some crowdfunding and payment companies have refused to allow donations going to groups supporting the Ukrainian military. Due to this, cryptocurrencies have emerged as a powerful alternative. £10.2m worth of Bitcoin has been sent to Ukraine by anonymous donators, making Bitcoin jump 13% and bringing it back on track from its slump. Big Tech companies have also answered Ukraine's call for help and stepped in to restrict Russia's state media and prevent further spreading of propaganda.

With restrictions placed on Russia, there is no doubt we will feel the repercussions of this war. Russia is the largest exporter of raw materials, gas, oil, metals, and wheat. Prices will likely surge as Russia increases their export revenues to boost its existing fiscal surplus and increase its financial reserves. There have also been predictions on an impact on pensions because of the crisis.

Due to the numbers of people fleeing Ukraine, Boris Johnson has announced a new humanitarian scheme allowing companies and citizens to sponsor individual Ukrainians to the country.

It is likely these announcements and actions undertaken will have a direct and indirect impact on fraud in the UK.

- **So What?**
- Inflation will be reflected in items such as fuel, but also metals, flour, bread, meat, and dairy, making the cost-of-living impact worse.
- Politics influencing the behaviour of larger cyber criminals and nation state linked actors.
- Increase in fraud reports connected to the crisis, for example, phishing and charity scams as well.
- There will be indirect scams through wider economic fallout, due to the knock-on effect of the crisis. For example, fraudsters will use phishing and vishing fraud purporting to be companies that can offer a better rate on their fuel bills.
- The Economic Crime Bill has been brought forward to act against Russians who raise funds in the UK. This may also increase money laundering out of the UK as a result.
- Increase in the price of Bitcoin leading to more investment in cryptocurrency putting people at risk of fraudulent investments.
- The new UK visa scheme could be open to abuse by people making fraudulent claims.
- Cyber-attacks aimed to disrupt the UK refugee scheme and operations.
- Scammers may set up fraudulent websites purporting to be legitimate sites registering details of those willing to house refugees. Phishing/Smishing could also increase as a result.
- Microchip shortages due to business operations suspended in Ukraine will have a knock-on effect on the goods that have them, leading to increases in prices and criminals exploiting consumers trying to obtain products.
- Increased demand for forged and falsely obtained genuine Ukrainian passports.
- Reports of a knock-on effect of the war on the value of people's pensions. Fraudsters could exploit people who withdraw pensions earlier and look to reinvest in alternative schemes.
- Exploitation by UK fraudsters of Ukrainian refugees looking to claim benefits in the UK.
- Potential increase in food fraud due to global supply disruption caused by the conflict.

Provenance:

Clampdown on Russian 'dirty money' in UK - Your Money

How the Ukraine crisis will affect your investments, petrol costs and energy bills - Your Money
https://www.aic.gov.au/sites/default/files/2021-04/rr19_fraud_and_its_relationship_to_pandemics_and_economic_crises.pdf

Russian websites down as Ukraine asks hacking groups for help (computing.co.uk)

Statement on the phasing out of Russian oil imports - GOV.UK (www.gov.uk)

Inquiry to look at whether reforms needed to combat 'horrifying' fraud levels | The Independent

Ukraine war: UK households offered £350 a month for hosting refugees - BBC News

Russian invasion of Ukraine: operational and cyber resilience | FCA

Ukraine invasion: Could Russia turn to cryptocurrency and cyber crime to dodge sanctions? | Science & Tech News | Sky News

Statement on corporate transparency and economic crime measures - GOV.UK (www.gov.uk)

Why the 1p income tax cut could knock £1,000s off your pension - Your Money

Why the war will impact your pension - Your Money

Immediate benefit support for those fleeing the invasion in Ukraine - GOV.UK (www.gov.uk)

Food fraud and the Ukraine war (foodmanufacture.co.uk)

UK defence minister orders inquiry into fake call from 'Ukrainian PM' | Reuters

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