NATIONAL FRAUD INTELLIGENCE BUREAU

MONTHLY THREAT UPDATE

June 2021

Overview of Fraud and Cyber Dependant Crime Trends

CITY OF LONDON POLICE
National Policing Lead For Fraud

Fraud and Cyber Dependent Crime Trends

Action Fraud Crime Reporting Volumes in MAY 2021

Reporting Volumes

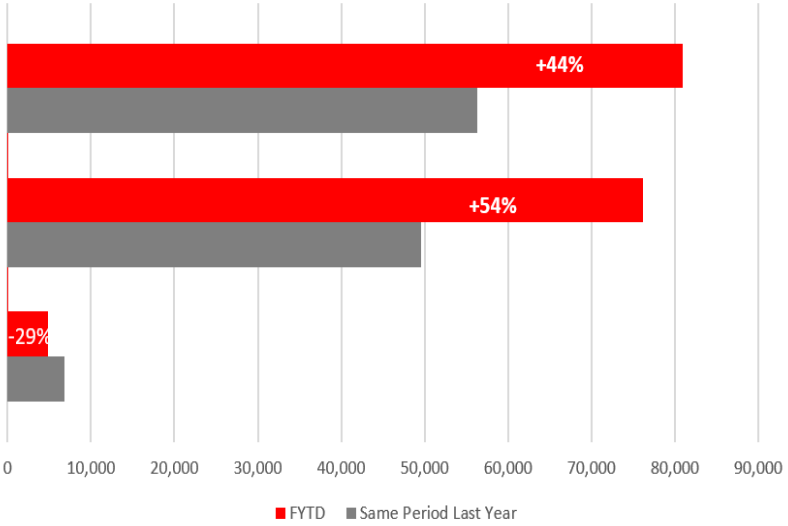
39,573 reports received

Fraud: 37,091

5% decrease compared to last month

Cyber: 2,482

6% decrease compared to last month



- Reporting (crime and information reports) decreased from 56,811 in April to 54,845 in May.
- Despite the drop in reporting, there was a rise in total losses from £197,193,601 in April to £302,251,015 in May.
- Dating fraud reporting volumes has increased once more after a drop in reporting last month and there has been an upward trend in losses since the start of the pandemic.
- Much of the increase in losses appears to be driven by losses to investment fraud, particularly in the 40-49 age group. Online shopping fraud reporting continues to drop in volume from its highest reporting in January. Mandate fraud[1] increased once more after a drop in reporting last month and losses are also increasing.
- Abuse of Position of Trust reports has increased once more to the highest levels since October 2020 and losses have also increased. Reports have been increasing steadily over the last few months and appears linked to lockdowns.
- Door to Door Sales fraud reporting has increased once more and is now at the highest levels since July 2019. Fraud Recovery reports remain high despite a slight drop last month. After a drop last month, Lender Loan fraud reports have increased once more. Rental Fraud is now at the highest levels since October 2020.

Observations

May's MO's: Websites purporting to offer gardening equipment, fitness equipment, investments, shipping containers, electronic products (phones and laptops), shutters, and driving licence renewals were common last month.

There were several reports received this month regarding victims trying to buy cars online. The cars were advertised for sale through a social media website or an online selling website. After the money is transferred contact is ceased and the car is never received. SMS texts are in circulation purporting to be from banks requesting that the recipient's mobile app needs to be verified via a link included to get the latest update on your account.

[1] Mandate Fraud is where fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer money to other accounts.

EMERGING ISSUES

DVLA Fake Emails: Over 1,300 reports have been received in one week regarding emails claiming to be from the DVLA. The emails claim that the recipient's vehicle tax is unpaid and there is a deadline of 5 working days to complete payment. The links in the emails lead to a genuine-looking DVLA website set up to steal personal and financial information.

Suspects Claiming to be from Action Fraud: Action Fraud have reported a scam circulating where criminals are contacting victims claiming to be from Action Fraud and requesting bank account and PIN details.

Pet Recovery Fraud: An emerging pet recovery fraud trend has been observed. The fraudster uses online platforms to identify people who have advertised that their dog or cat is missing. The fraudster tells the victim that they have their pet, or know where it is, and requests funds for its safe return. If the victim is reluctant to make the payment, they threaten that they will harm the pet. Because the fraudster obtains the victim's contact details from the internet, they can target victims from various parts of the country, regardless of their own location. 28 reports have been recorded this year, and the total loss is £3,925.

Mobile Phone Upgrade Scam: The NFIB are aware of an ongoing scam where consumers are being cold called by individuals impersonating employees of legitimate mobile network operators and suppliers. Victims are offered early handset upgrades, or new contracts, at significant discounts. Once customers have been convinced that the deals are genuine and agree to proceed, suspects then ask for their online mobile account credentials, including logins, address, and bank account details. Suspects then place orders with genuine companies on behalf of victims, however select a different handset to that requested and have it shipped to the customer's address. Upon receipt, suspects assure victims that this has been an error and instruct them to 'return' the handset to a different address not affiliated to the mobile company. These addresses are usually residential. Upon intercepting the 'returned' handsets, the suspects cease contact and victims find themselves stuck with no phone and liable for the entirety of a new contract taken out in their name. The NFIB have received over 300 reports since January 2020 with reported losses more than £86,000.

Covid Digital Passport Scam: A new email scam about Covid is currently in circulation. The email purports to be from the NHS and informs recipients that they can apply for their 'Digital Coronavirus Passports' through a link. The link takes the user to a fake NHS website which requests personal and payment details.

Scams warning for tax credits customers: HMRC have warned tax credits customers to be wary of tax scams as the remaining annual renewal packs arrive in the post this month. Anyone doing their tax credits renewal who has received a tax or benefits scam email, or text might be tricked into thinking it was from HMRC and share their personal details with criminals, or even transfer money for a bogus overpayment[2].

[2] Scams warning for tax credits customers - GOV.UK (www.gov.uk)