NATIONAL FRAUD INTELLIGENCE BUREAU

MONTHLY THREAT UPDATE

March 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 February 2021

Reporting Volumes

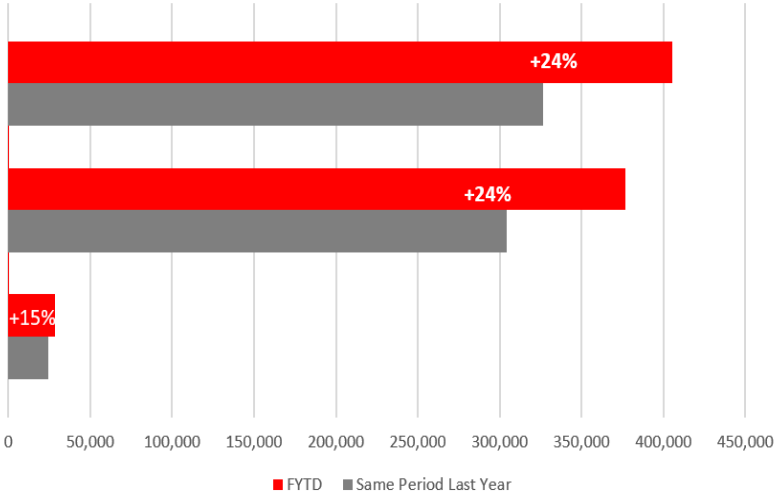
47,735 reports received

Fraud: 45,403

18% increase compared to last month

Cyber: 2,332

9% decrease compared to last month



- Reporting (crime and information reports) increased from 57,701 in January to 64,356 in February.
- Total losses increased significantly from £173,112,979 to £286,562,188 in February. This represented an average loss of £4,908 per victim.
- Dating fraud reporting increased again by 15% from 640 to 649 crime reports and are at the highest levels since reporting began.
- Investment fraud reports have risen significantly in February, share sales have gone up to high levels again (645 reports) and Other Financial Investments have climbed and are now at the highest levels since reporting began (1157 reports).
- Fraud Recovery have jumped to the highest levels over the past two months (203 reports). Pyramid and Ponzi scheme reports remain at high levels (211 reports) and Other Advance Fee reports (3047) have been climbing again after the drop in December. Consumer Phone Fraud has continued to increase since it reached its highest levels in January (649 reports).
- Ticket Fraud reports are now at the highest levels since March 2020 (216), likely due to the announcements around relaxations in restrictions.

Notable Reporting Trends

Cyber Trends: The Education sector has been identified as a prominent target for exposure to cyber-attacks with an increase in reports over the past year, 16.6% up on the previous year. Schools accounted for over a third of reports in the last year. A shift to remote working and online learning saw a rise in reports of hacking/bombing of virtual learning environments. Social media and email hackings accounted for 34% of total reports in the last year (80 reports), followed by Computer Virus and Malware offences (61 reports). Educational organisations remain a viable target for cyber criminals as cyber security measures vary and some targets have limited measures increasing their risk of falling victim.

Royal Mail Scams: Scammers are sending fake emails purporting to be from Royal Mail claiming they were unable to deliver people's packages. These emails claim delivery was attempted but there was no one in to take the package along with a link leading to fraudulent websites, which recipients are asked to click on to reschedule their delivery and this provides an opportunity for fraudsters to steal personal details and financial details.

NCA or National Insurance Scams: Victims are reporting receiving calls from either the NCA or 'National Insurance' claiming that the vehicle which has been registered to them has been found with drugs in it and because of this the vehicle has been seized and their National Insurance has been frozen. They are told they need to pay a given amount of money and are given the account details of supposed police officers who are investigating them.

OBSERVATIONS

February's Online Suspect Websites: Websites purporting to offer investments and driving licence renewals were common last month. A significant number of reports received relating to online shopping fraud were websites selling home appliances and kitchen products, shipping containers, gaming consoles, white goods, shipping containers, and exercise equipment.

February's MO's: Individuals searching for an ISA online and contacted by a company purporting to be a genuine company. They are requested to complete a form with personal details and documentation before being asked to pay money to invest. The victims then realise that another company has been cloned. Individuals buying fake flight tickets are starting to increase once more.

EMERGING ISSUES

Holiday Fraud: NFIB have issued an alert to warn members of the public about the risk of holiday fraud and ticketing scams following the government's announcement of the road map out of lockdown. Any significant demands for holidays are likely to be exploited by scammers leading to an increase in holiday fraud.

Festival/Concert Ticketing Fraud: Some organisers have announced that events will be going ahead this summer. Following this announcement there has been a huge demand for tickets, with some festivals, such as Leeds/Reading Festival selling out quickly. Action Fraud have started to see reports of ticketing fraud as people who missed out on the official websites, search for tickets from other sources. We would expect to see reports significantly increase over the coming months.

EMERGING FRAUD THREATS

Budget: The Chancellor made several announcements in the Spring Budget 2021 which may impact on the fraud picture. Extension of the furlough scheme until the end of September 2021 and support for COVID-19 hit sectors, including a new Recovery loan scheme and a Restart Grants scheme could be exploited by fraudsters. However, fraud will be tackled in COVID-19 schemes through investment of £100 million in a new HMRC taskforce.

Contactless card limit will rise to £100. Although contactless fraud is small at present, the number is likely to increase as contactless spending frequency increases.

Household Spending Increase: report by the Centre for Economics and Business Research (CEBR) suggests that a quarter of the £192 billion saved during lockdown will be spent. Scammers will be keen to exploit this uptake in spending and will use numerous methods and scams to get individuals to hand over cash.

Easing of Lockdown Restrictions: As lockdown measures are eased, it is likely that we will see movement in volumes relating to certain fraud types. For example, volumes of reports relating to holiday scams and ticketing fraud are likely to increase once more. It is unclear what will happen to online shopping fraud because of easing of lockdown restrictions. We may see a significant decrease in online shopping fraud as shops and services open once more, however, it is noted that online buying behaviours may have changed because of the pandemic, therefore, online shopping scams may continue to be higher than prior to lockdown.

Vaccine Supply and Distribution: Recently, there have been news reports on apparent shortages in the vaccine supply distribution. Any reported shortages are likely to play on people's worries about not receiving vaccinations which make them vulnerable to falling for vaccine scams. These scams such include phishing emails and adverts for sales of non-existent vaccines.

COVID-19 19 Vaccine and Testing Certificates: There is the potential for vaccine and testing certificates as well as immunity passports, mobile travel health passports and apps which could be exploited by scammers. Any potential databases containing details of vaccinated individuals are susceptible to cyber-attacks, hacking and data theft.