cifas
The UK's Fraud Prevention Community

FRAUDSCAPE 2021

KEY FINDINGS

OVERALL

2020 was one of the most challenging years we have faced, yet Cifas members still recorded 309,849 cases of fraudulent conduct to the NFD, which is one case every two minutes.

Despite the pandemic and economic situation impacting filing volumes, the first six months of 2021 do show a 13% increase in the number of cases recorded to the NFD compared to the same period of 2020.

Facility takeover grew significantly last year, with the number of cases recorded rising by 21% on 2019.

Despite lower levels of recruitment, there were notable filings of dishonest actions and disclosing personal information to third parties.

Identity fraud and misuse of facility were important challenges, accounting for 82% of the total cases recorded in 2020.

IDENTITY FRAUD

185,578 cases were recorded in 2020, which is a 17% reduction compared to 2019. However, the first six months of 2021 do show a 11% increase on the same period in 2020.

A large proportion of identity fraud victims were aged between 31 and 40 years and 51+.

The plastic card and banking sectors were the most affected, with a slight rise for online retail.

2020 also saw a 23% increase in companies being impersonated. This may be due to the abuse of stimulus package offerings aimed at supporting businesses through the pandemic.

MISUSE OF FACILITY

68,083 cases of misuse of facility were recorded last year, which, despite the 19% reduction from 2019, still accounts for more than a quarter of cases recorded. However, the first six months of 2021 do show a 23% increase on the same period in 2020.

A high proportion of adults aged 21 to 30 years were identified in cases where intelligence indicates mule activity.

The main product overwhelmingly targeted for misuse is bank accounts, which make up just over three quarters of misuse cases. 78% of cases involving the misuse of bank accounts have intelligence that indicates money mule activity.

There was a 26% increase in misuse of company accounts, which may be linked to the abuse of stimulus packages.

FACILITY TAKEOVER

38,421 cases were recorded last year, which is a 21% increase compared to 2019. However, the first six months of 2021 do show a 14% increase on the same period of 2020.

41% of products are taken over within two weeks of the product being applied for. This is highly prevalent for bank accounts and telecoms products.

44% of cases were carried out via telephony channels, and there was a 22% increase in this type of activity suggesting that there may be a perception that telephony channels are weaker.

INSIDER THREAT

290 individuals were recorded to the IFD in 2020 compared to 432 in 2019. However, the pandemic has limited recruitment and new risks have emerged with remote working.

The pandemic has had a significant impact on employment, with 693,000 payroll jobs lost since March 2020.

Dishonest actions remained the highest reported case type, accounting for 44% of cases.

Cases recorded for unlawful obtaining or disclosure of personal data have risen by 43%. The individuals involved tended to be aged between 31 and 40 years and working in a branch or a store.

SUMMARY

Much of the impact of COVID-19 on fraud is still to be seen. Perpetrators are highly likely to exploit a range of vulnerabilities and uncertainties, including employment scams, travel scams and investment fraud, as well as the stimulus packages on offer.

The impersonation of companies throughout the pandemic means it is highly likely companies will be increasingly targeted if further provision is offered to business to support the economy.

Identity fraud remains a priority for all sectors, due to the rise of synthetic identities and readily available access to false documentation.

The rise in cybercrime as a service, such as phishing kits, fraud tool kits and hacking services, is an extremely high threat to all sectors.

Social media continues to be a key enabler for recruiting mules with more than two thirds of the UK population using a social media platform.

The pandemic has changed how mules “cash out”. Cashing out via cryptocurrency assets and wallets has become attractive to criminal networks due to the anonymity this provides.

Facility takeover has seen a significant rise during the pandemic. It is highly likely that digital channels will continue to be favoured but as organisations bolster their defences, threat actors may look to exploit vulnerabilities via telephony channels.

Remote working remains a threat and so it is essential that organisations review their working from home policies and audit the data and information that staff have access to.

Economic uncertainty as a result of the pandemic may put financial strain on employees who then may justify carrying out certain activities for financial gain. It is essential to screen staff not just at application, but throughout employment.

The UK's Fraud Prevention Community

CONTACT US

For any press enquiries please contact
press@cifas.org.uk

If you are interested in joining Cifas
click here

For more information about our
Fraud and Cyber Academy
click here