Long Covid: dishonest consequences

*The economic crime impact of Covid-19 is incalculably greater than even the most accurate estimates of losses to wrongful claims on government support schemes: the lockdowns drove everyone online, suggesting new opportunities to gain at others' expense, whether at work remotely, perhaps merely by loaning personal credentials for a fee or as a social engineer to steal the same and access accounts. **Paul Cochrane** looks at the legacy effect of the pandemic on fraudulent behaviour as well as how it is affecting a specific demographic.*

Treasure hunt

RELATED ARTICLES

Silver lining? - recruitment survey

Unentitled – a global look at false claims for Covid-19 support

How immune are Covid-19 relief scheme fraudsters?

Pandemic predators – Covid-19 fraud schemes

Scale, breadth, response – fraud online

Fraud has spiked since the outbreak of Covid-19 and is still on an upward trajectory as economies struggle to rebound from the pandemic, according to research by Grant Thornton and the US-based Association of Certified Fraud Examiners (ACFE). [1] One of the biggest growth areas in fraudulent activity, according to the American Bankers' Association (ABA) is exploitation of the elderly, particularly in ageing societies such as the USA, Europe and the east Asia.

Boom time

Across the world, fraudulent activity has risen since 2020, said the ACFE, with 51% of organisations worldwide uncovering more fraud than usual since the pandemic began (survey data was gathered between May 2020 and May 2021), with "one-fifth indicating a significant increase in fraud."

In the US, consumer fraud losses reached a new high of US$5.8 billion in 2021, a 70% increase on 2020, according to the USA Federal Trade Commission [2], while 'smishing' – whereby a perpetrator texts a victim posing as a legitimate business to gain access to personal information and money – was up 58% over the same period. [3] In the UK, SMS 'phishing' attempts increased by 700% in the first six months of 2021 compared to the latter half of the previous year, according to UK consumer watchdog magazine Which?. [4]

Gone phishing

"Recently, we've seen a huge push in phishing and [targeted] spear-phishing attacks that work around two-factor authentication. Fraudsters posing as customer service agents or other officials might request your login details via SMS, DM (direct messaging), or even a chat box in an existing platform or video game. Lots of resources go into writing malicious scripts that send the phishing message, then hack the associated account in real time," said Gergő Varga, a sales content manager at SEON Technologies, a UK-based fraud detection and prevention software company.

At the same time, Tom Caulfield, co-founder and chief operating officer at Procurement Integrity Consulting Services in Virginia, USA, argued there had been no emergence of a brand-new fraud technique since Covid-19 exploded around the world in February 2020. "A scheme is a scheme. What has happened is the pandemic accelerated the speed of fraud and corruption globally... knowing the hundreds of millions that was spent in emergency contracting during Covid response," he told *FI*.

Ever the opportunists

The pandemic did, however, force a change in criminal activity, said Mark Anderson, director of training and development at Investigative Associates, in Pennsylvania, USA: "There has been a bit of a reset, especially if fraud involved contact with people, as fraudsters lost their customer base during the pandemic," such as door-to-door swindles. "If criminals were existing off fraud, they either modified their approach or did something different," such as moving into cybercrime and identity fraud. "Fraudsters are very much creatures of opportunity, so if the pandemic put a blip in it, they re-tooled and did something else. I don't think a lot of fraud has gone down, it has just been modified or replaced by what is more lucrative," said Anderson.

Personal worth

With a post-Covid economic hangover prompting recessions around the world, Varga noted that during economic downturns there is often an uptick in criminal innovation: "Right now, the vertical under attack is identity verification (IDV). Deepfake technology makes IDV more complicated, even for liveness detection via video stream. As inflation is on the rise, more people are willing to participate in money muling schemes, opening up bank accounts just to hold and transfer illicit funds, or even simply handing over their personally identifiable information (PII) and biometrics – ID and face – for fraudsters to beat IDV," said Varga.

Anti-fraud professionals noted a spike in identity fraud to access government grants and financial support during the pandemic. Financial support was distributed "so fast there were little to no internal controls. The government is facing all this fraud from the pandemic in every walk of life, with one of the largest frauds the use of fake IDs to get as much free money as possible," said Sheryl Goodman, president and co-founder of the Procurement Integrity Consulting Services.

Indeed, the US government provided some US$6 trillion in emergency spending through the pandemic, with officials from the White House admitting that immense fraud took place, particularly in small business loans and unemployment insurance [5], with some US$4.5 billion in over-paid grants made to self-employed workers and US$4.5-6 billion defrauded from the unemployment insurance programme.

More or just more productive?

What is puzzling anti-fraud professionals, particularly in the USA, is whether government handouts and stay-at-home measures during the pandemic have led to an increase in the number of fraudsters, or if old hands have increased their fraudulent practices. "The giveaway programmes have gone, so did people get that much money [from the government]? Or did sitting at home for two years, and not wanting to work, make an impact [on fraudulent activity]? That question is still out there," said Goodman.

Anderson also questioned whether an uptick in fraud may be underway. "What do people do for money when the Covid funds dry up and they don't have the concept of right or wrong, or don't want to work? They may turn to fraud," he warned.

While remote fraud is a clear and present danger, so is remote working, said Caulfield.

"As people are working from home, the reporting of [fraud] complaints [within companies] has reduced and there is less oversight. It is scary how a company might not see potential fraud, as if there is no reporting going on, it doesn't mean there's no fraud happening.

"Companies are getting complacent, which could be an issue going forward," he observed.

All about me

Another concern that has emerged from the pandemic is a growing behavioural trend by fraudsters to intellectually rationalise crime: "People are going to be more aggressive in committing fraud due to the rationalisation of entitlement – I was a financial victim of Covid-19 and no fault on my part, or I didn't get financial support because of the way legislation was written. And the lack of, or reduced oversight, due to remote working gives them greater opportunity to commit a fraud. That is probably something inherent in a global crisis situation," said Caulfield.

Anderson also noted a rise in the "concept of entitlement" and narcissism when he was interviewing fraudsters: "The biggest behavioural issue is a societal one, that of self-focus and narcissism. From an interview point of view, to get people to tell me why they committed a crime, you don't appeal to what their family or others might think, it is only about how they [the perpetrator] feels. They feel that they've built the fraud and own it, so a self-focused crime, and they will protect that fraud. It is almost approaching how psychopaths and sociopaths think – that others don't matter. And fraudsters think they are smarter than the investigators. This behaviour concerns me, and it will explode even more as there are so many opportunities to make it happen," warned Anderson.

A vulnerable age

Indicative of this trend is the rise in fraud targeting the elderly, including by family members and other trusted associates. According to a report [6] by the AARP (formerly the American Association of Retired Persons), the rate of elder financial exploitation (EFE) has more than doubled since the start of the pandemic, while EFE by trusted others has increased by two to three times globally.

In the US, elder-targeted fraud perpetrated by trusted others rose from 3.5% pre-pandemic to 7.5% during the pandemic, while in China the rate of this crime rose from 2.6% to 6.8%.

In Canada, estimates show an increase in elder abuse of 250% percent, primarily financial and physical abuse, the report noted.

In the US, fraud by trusted others includes scams focused on guardianships, which is a fiduciary relationship between one person (the guardian) and a ward to act on their behalf. Said Anderson: "A huge area where fraud is skyrocketing is in guardianships, as due to the baby boomer generation there are so many elderly. This fraud is either by people trying to get into guardianship, with people trying to get into the business with the intent to divert funds for their own use, or by fraudsters going after guardians to take advantage of their fiduciary responsibility," said Anderson.

Guardians may be targeted, he added, as they are publicly listed, enabling fraudsters to know a potential target. Schemes targeting the elderly and guardians are like frauds designed to target other demographic groups, but with an emphasis on playing on vulnerability.

"There are many schemes, such as sales – the roof is falling down and needs to be repaired – to Ponzi schemes," where the dishonest target the elderly. "Old school simplistic crimes go on all the time, and the guardian is not always around," said Anderson.

Other fraud techniques targeting the elderly include romance frauds, which have surged in recent years, with US$547 million stolen in the US in 2021, more than five times in 2019, according to the Federal Trade Commission's Consumer Sentinel Network. The median loss to the elderly, at US$9,000, was 92% higher than in the 18 to 29 age group. [7]

Peer-to-peer (P2P) payments are another fraud area of concern, with P2P fraud having surged prior to the pandemic, by an estimated 733% between 2016 and 2019, across all ages, according to US-based Javelin Strategy & Research. [8] "Older adults are engaging with new technologies, which also introduces the potential for new exploitation methods," noted the AARP report.

Awareness around the issue is rising, with the US' National Guardianship Association certifying investigators to root out such fraudulent activity, noted Anderson. "With the ageing of the world's population, one will see fraud targeting the elderly more and more," he predicted.

Notes

1. https://www.grantthornton.com/content/dam/grantthornton/website/assets/content-page-files/advisory/pdfs/2021/next-normal-preparing-post-pandemic-fraud-landscape.pdf
2. https://www.aarp.org/money/scams-fraud/info-2022/ftc-fraud-report-new.html
3. https://www.aarp.org/money/scams-fraud/info-2020/smishing.html.
4. https://press.which.co.uk/whichpressreleases/smishing-attacks-in-the-uk-grew-by-nearly-700-in-the-first-six-months-of-2021-which-reveals/
5. https://www.washingtonpost.com/us-policy/2022/02/17/stimulus-aid-oversight-fraud/
6. https://www.aarp.org/content/dam/aarp/money/scams_fraud/2022/10/aarp-banksafe-pandemic-report-10-3-22.pdf
7. https://www.aarp.org/money/scams-fraud/info-2022/ftc-report-romance-scams.html.
8. https://javelinstrategy.com/research/2020-identity-fraud-study-genesis-identity-fraud-crisis

Nov 10 2022

Print this page | Send to a colleague | Email the Editor

Comments

TOPIC ALERTS

Psychology & Profiling
Comment, Surveys and Research
Identity Fraud
Online Fraud
Frequency: Daily
No. of articles: up to 10
Email Address: timon.molloy@informa.com
Manage topic alerts | Set up Alert

ONLINE FRAUD

Europol leads fight against 'police ransomware'
Stories, analysis, statistics – April/May 2011
Stories, analysis, statistics – December 2010 / January 2011
ENISA calls for EU forum to fight virtual world fraud
'Click fraud' on the rise in US Internet advertising market
UK card not present fraud rises sharply

COMMENT, SURVEYS AND RESEARCH

Huge public procurement losses to corruption, says OLAF
Public services fraud rises in England
Customer is banks' first line of detection, study reveals
Smartphone users more likely to be victims of fraud
Corporate payments prime target for fraud, survey finds
Cybercrime second most reported economic crime in financial services

IDENTITY FRAUD

Stories, analysis, statistics – April/May 2010
Identity theft flat, but other trends up
EU passport timetable set to clash with US
Europe set to clash with US over biometrics deadline
Fingering illegal entrants
Driven to consistency

PSYCHOLOGY & PROFILING

Stories, analysis, statistics – August/September 2011
Who lies to obtain financial products?