PUBLIC PRIVATE ECONOMIC CRIME NEWSLETTER

Issue 5 | July 2021

Introduction

Welcome to July's edition of the Public Private Economic Crime Newsletter. This edition looks at the recent G7 summit, and preparations for September's meeting of the Interior Ministers.

It explores the inaugural meeting of the Suspicious Activity Reports (SARs) Advisory Group, and the National Economic Crime Centre's (NECC) public private threat groups, and we look at the information sharing pilot.

In the latest of our 'explained' series we look at the Fraud Action Plan.

UK's G7 Presidency

HM Treasury's G7 work culminated with Finance Ministers in early June committing to introducing and strengthening company beneficial ownership registries to better tackle the illicit finance generated from environmental crimes, corruption and other organised crime.[1] We are pleased that the US, Canada and Japan are now also implementing registries. Finance Ministers also pledged increased financial and human resources to the FATF style regional bodies, with at least US$17 million and 46 assessors over 2021-24. This is to improve global implementation of the FATF's AML/CTF standards.

The Home Office's Joint Anti-Corruption Unit (JACU) is preparing for the G7 Interior Ministers' meeting in September.

The meeting of the G7 Ministries responsible for internal affairs will include discussions on strengthening international action against corruption, and kleptocracies.

JACU also worked with G7 partners on a joint statement for the UN General Assembly Special Session Against Corruption[2], highlighting priorities including civil society engagement, transparency, and beneficial ownership. Anti-corruption also features in the G7 Leaders' Communiqué[3] and Open Societies Statement.[4]

Suspicious Activity Reports (SARs) Advisory Group

Comprising membership from the public and private sectors, the SARs Advisory Group will act as a continuous improvement mechanism for the effectiveness of the SARs regime. At the inaugural meeting (27 May), the Group agreed to take forward three initial work strands to build an evidence base for change: the characteristics of a SAR that make it more likely to provide intelligence and operation opportunities; maximising asset recovery from Defence Against Money (DAML) SARs; and improving the quality of SAR reporting in sectors that typically report fewer SARs.

For the duration of the SARs Reform Programme, the Advisory Group will align its more operationally focused work with the strategy of the Programme (via the Programme Board) and will monitor the impact of the changes implemented as a result its recommendations.

[1] Finance track communique
[2] G7 UNGASS statement - GOV.UK (www.gov.uk)
[3] Carbis Bay G7 Summit Communique (PDF, 430KB, 25 pages) (g7uk.org)
[4] 2021 Open Societies Statement (international.gc.ca)

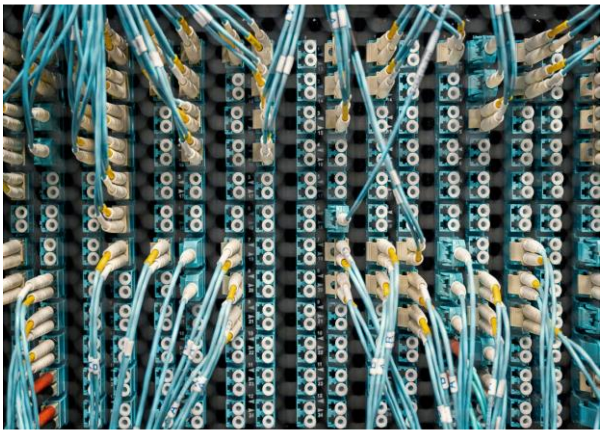
‘Phishing attempts soar amid pandemic’

Since the Suspicious Email Reporting Service (SERS) was set up in April 2020 by the National Cyber Security Centre and the City of London Police, more than 43,000 email scams have been identified and 84,000 websites have been removed from the internet. As of April 30, this year, 5.8 million reports of phishing emails had been received into SERS.

The most common fake organisation reported in phishing emails was TV Licensing, with victims reporting losses totalling £5.3 million – an increase of 118 per cent compared to the previous financial year. The next most common faked organisations were HMRC and DVLA, and more than 40,000 COVID-19 related emails were also reported into the SERS by members of the public.

Action Fraud, the national reporting centre for fraud and cybercrime, also received over 146,000 reports of suspicious messages by phone calls and text messages in the 2020/21 financial year – an increase of 80 per cent on the previous financial year.

The publication of these figures came as the National Fraud Intelligence Bureau’s Cyber Protect team launched a national awareness campaign on June 1 to remind the public to think twice before handing over personal and financial information as a result of a suspicious message.



Private to private information sharing pilot

Private sector institutions report facing uncertainties sharing information with each other quickly, meaning they often only see their part of the puzzle. This risks undermining the quality and comprehensiveness of SARs reporting, which means that criminals who are exited or refused a service from one institution for financial crime reasons can continue to exploit the system through different service providers, displacing crime rather than disrupting it. This also creates an additional risk that innocent parties are reported to law enforcement.

A pilot, which will run for 6-9 months within the Information Commissioner’s Office regulatory sandbox, will explore the extent to which regulated entities can share information where it is conducting, or has conducted, a targeted money laundering investigation.

The aim of the pilot is to test how far the current regulatory framework allows information sharing for the purposes of combating money laundering and advise on any necessary changes.

Public Private Threat Groups (PPTG)

PPTGs on Fraud, Money Laundering, Terrorist Financing and Tax Crime and Evasion have been created under the new NECC JMLIT+ operating model.

Public private threat-based activity is now being conducted underneath the PPTGs in ‘Cells’ which are time-limited groups with specific and measurable objectives.

There are currently thirteen Cells across the PPTGs, which are focusing on delivering disruptive activity against the 4P[4] response to economic crime threats.

In the last quarter the JMLIT+ Cells published six alerts, which raised awareness of crime typology red flags and have allowed private sector partners to conduct crime prevention activity through changes to their processes.

A recent example of a cell delivering threat response activity is ADMIRALTY which is focussed on the money laundering threat through post office accounts. The cell has used public and private intelligence to coordinate operational activity resulting in four arrests and £169,000 being seized.

Forward Look

Public Private Operational Board	Wednesday 14 July 10:00-12:00
SARs Advisory Group	Wednesday 29 September 13:30-15:00
Public Private Steering Group	Thursday 30 September 11:30-13:00

Contact

If you would like to contribute to a short article or a news article for the next edition, please do not hesitate to get in touch at:

HOECSET@homeoffice.gov.uk

[5] Protect, Pursue, Prevent, Prepare

FRAUD ACTION PLAN EXPLAINED

What is the problem?

Fraud is the most common crime, now accounting for almost 37% of all estimated crime in England and Wales. The increasingly digitalised economy offers growing opportunities for criminals, with insufficient defences or disincentive.

What needs to change?

Fraud affects everybody and that’s why the public sector, law enforcement, and the private sector are all working towards better protecting the public and businesses from fraud, reducing the impact on victims and ensuring that fraudsters have no safe space to operate.

What is the approach?

As set out in the Economic Crime Plan Statement of Progress[5] the February 2021 Economic Crime Strategic Board, approved a draft framework for a Fraud Action Plan to be published following the 2021 Spending Review. Under five pillars (set out below) the Plan will include all key stakeholders and identify actions that will remove the vulnerabilities that fraudsters exploit, shut down known fraudulent infrastructure, identify and bring the most harmful offenders to justice, and crucially ensure the public have the advice and support they need.

1. Restrict opportunity

This involves strengthening of industry collaboration with government by relaunching the Joint Fraud Taskforce as a Ministerial-chaired forum, focused on outcomes that protect the public. It also looks at enhancing our public-private partnership approach to fraud by developing sector charters with industry to design out fraud at source.

2. Disrupt the market

This pillar looks at how we can disrupt the market by giving resources and capabilities to agencies such as the National Cyber Security Centre to undermine online fraud infrastructure.

3. Improve intelligence

This looks to improve the way we gather and exploit intelligence through a new, and improved, Action Fraud as well as more sophisticated data and covert intelligence capabilities.

4. Arrest the biggest players and increase enforcement

This pillar looks at how we can go after the big players by giving the National Crime Agency and the Regional Organised Crime Units the resource they need to go after those committing the worst types of fraud. It also seeks to push more fraud cases through the criminal justice system, whilst working with the private sector to crack down on money mules.

5. Safeguard victims and change public perceptions

This pillar addresses how we can ensure that the public have the advice and tools they need to protect themselves, whilst ensuring victims have the support they require.

[5] Economic crime plan 2019 to 2022 - GOV.UK (www.gov.uk)