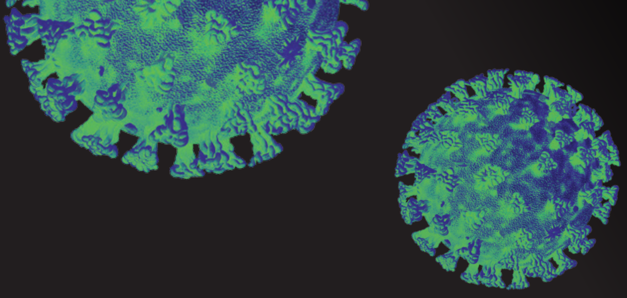
Government
Counter Fraud
Function



GOV.UK/coronavirus

COVID-19 Counter Fraud Response Team

NEWSLETTER

Issue #1 / April 2020

Welcome to our first edition of the COVID-19 Counter Fraud Response Team's newsletter. In our newsletter, we aim to:

1. **Keep you informed of the COVID-19 Fraud and Compliance Landscape**
2. **Introduce you to our most recent developments and implementations**
3. **Help you to ensure funding goes further, maximising support for the community**

The COVID-19 Counter Fraud Response Team has been established to proactively monitor the COVID-19 fraud threat utilising expertise, intelligence and analytics from its partnerships across sectors, including law enforcement, the public & private sectors as well as international partners through the Five Eyes. We are combining shared intelligence with expert fraud risk assessment of the stimulus spend, so we all understand the risks from fraud and the possible responses.

In addition to supporting public bodies to reduce the threat from fraud, we are developing a number of tools to help identify and resolve error and compliance issues with the government's stimulus spending.

All of these will help public bodies get the most out of the stimulus packages, and their business as usual funding streams, which are coming under increased demand at this time.

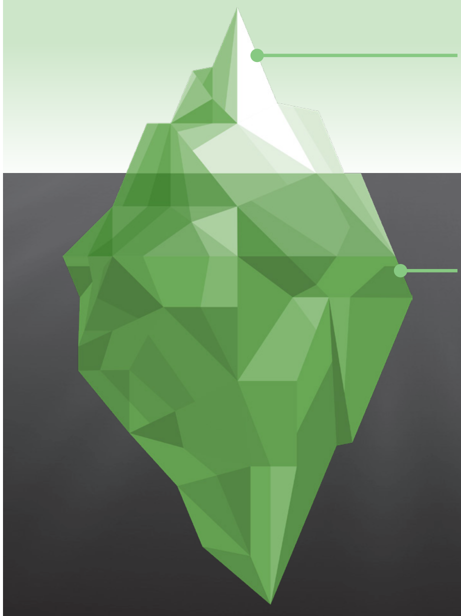
Mark Cheeseman
Director, Public Sector Fraud

COVID-19 Challenge Update

We do know that fraudsters are using COVID-19 specific scams to exploit the public. We have identified that the majority of these have been related to **phishing, malware, bogus caller and online shopping scams** where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived. In addition, fraudsters have also **impersonated Government officials** such as HMRC, offering citizens a tax refund and directing victims to a fake website to harvest their personal and financial details.

Total COVID Stimulus Spending
£420 billion

Potential fraud & error loss
£2-£21 billion



Detected

The tools created & deployed by the COVID-19 Counter Fraud Response Team across departments and local authorities are already detecting fraud and error, stopping payments before they are issued. This is just the tip of the iceberg.

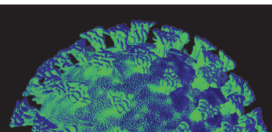
Raising the iceberg

To prevent further losses, as well as detect and recover fraud and error after the event, the COVID-19 Counter Fraud Response Team are using risk assessments at process design stage, as well as post-event assurance work to check for instances of fraud and error. Once identified these are then recovered via clawback agreements.

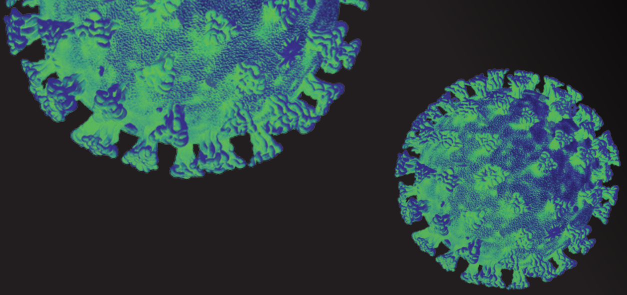
The Government has announced COVID-19 Stimulus Spending of around £420bn in 57 programmes administered by over 400 local authorities and 14 government departments.

£2-£21bn based on 0.5%-5% calculation based on government measurement exercises.

You can contact the Government Counter Fraud Function by emailing
covid19-counter-fraud@cabinetoffice.gov.uk



Government
Counter Fraud
Function



GOV.UK/coronavirus

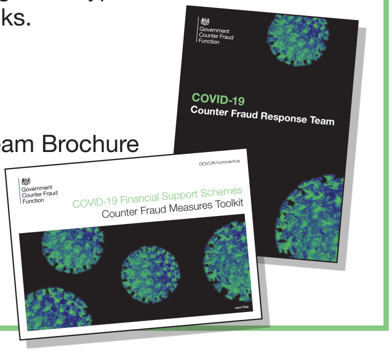
COVID-19 Counter Fraud Response Team

COVID-19 Counter Fraud Response Team Update

- **Counter Measures Team** has developed a bank account verification tool to enable Public Bodies to confirm they are paying a grant to the correct bank account using commercial and consumer credit data. The tool has been developed in collaboration with Experian and nine UK Banks. In addition to validating the account at source, the tool can also append financial information about the company - further building confidence that a legitimate business is being paid. The tool is available to Central and Local Government users and has gone live w/c 20th April.
- **Risk & Research Team** has completed Fraud Risk Assessments (FRAs) across all 53 COVID stimulus programs. This has allowed us to prioritise those that should now have detailed FRAs completed and the first seven of these have now been completed.
- **Governance and Stakeholder Engagement Team** have worked with NCA to establish direct intelligence sharing for COVID-19 via a network of SPOCs across the public sector to ensure emerging risks are flagged within 48 hours.
- **Capacity & Guidance Team** have issued guidance, fraud awareness materials, toolkits and more across 62 government bodies and all local authorities. Continuous capacity assessments are tracking the impact of COVID-19 on resources and as a fraud driver to both existing fraud types as well as new COVID specific attacks.

More information about how we can support you is available in our Team Brochure and Counter Measures Toolkit.

Get in touch for your copy!


Government Counter Fraud Function
COVID-19
Counter Fraud Response Team
GOV.UK/coronavirus
Government Counter Fraud Function
COVID-19 Financial Support Schemes
Counter Fraud Measures Toolkit

What is happening this week:

National Cyber Security Centre (NCSC)

National Cyber Security Centre

The NCSC have observed a rise in the use of COVID-19 related themes in **cyber crime** due to an increase in home working which has led to the use of more vulnerable services such as Virtual Private Networks (VPNs). In the UK, the NCSC has detected **more UK government branded scams relating to COVID-19 than any other subject.** NCSC have detected a number of threat actors that have used COVID-19 related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked web page. When they open the attachment the malware is executed, compromising the victim's device.

Cyber Aware

As a result, on Tuesday 21 April the NCSC, working alongside the **Home Office**, the **Cabinet Office** and the **Department for Digital, Culture, Media and Sport** (DCMS), will launch **Cyber Aware**, a refreshed campaign which aims to help individuals and organisations protect themselves online.

- **Cyber Aware:** The core message of the six most important things people can do to stay safe online.
- **Suspicious Email Reporting Service (NCSC and City of London Police):** Members of the public can report emails they consider suspicious and if found to be malicious the NCSC will take down associated websites.
- **Takedown statistics from their Active Cyber Defence (ACD) programme:** The number of COVID-19 related sites that have been taken down in the past month.
- **Video conferencing guidance:** New guidance to help individuals and organisations secure the use of video conferencing services.

The NCSC have also **published a joint advisory** with the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), providing information on the current exploitation by cyber criminal and **Advanced Persistent Threat (APT)** groups as well as a list of indicators for detection as well as mitigation advice.

Five Overarching Principles

The following principles have been developed to effectively control the levels of fraud in emergency management contexts:

- Accept there is a high fraud risk
- Integration of fraud control resources into process design
- Implementation of low friction counter measures
- Carry out targeted post event assurance
- Control framework re-assessment following move from emergency mode

You can contact the Government Counter Fraud Function by emailing
covid19-counter-fraud@cabinetoffice.gov.uk