Business Fraud Network

Regular updates on new and emerging fraud threats

Love business Hate fraud

TUESDAY 30 AUGUST 2022

In this update we highlight emerging fraud threats to businesses (especially SMEs) and offer practical advice on prevention. It is based on pooled intelligence shared by members of our Business Fraud Network which meets every six weeks.

We encourage all businesses – and everyone who works with them or otherwise supports them – to read, share and act on these updates.

CURRENT RISKS

- Action Fraud received 4,000 fraud reports from business in July (up 56% on last month). Most were from large businesses; one-in-four were from SMEs (10 – 250 employees). The most common frauds reported were bank fraud, mandate fraud, retail fraud and application fraud. Mandate fraud accounted for 5% of all business reports.
- There were 800 reports of corporate employee fraud in 2021/22. Reported losses totalled about £300m. Most reports were received from the retail, finance, insurance, healthcare, social work and construction sectors.
- Action Fraud received 110 cybercrime reports from business in July. Of these, 71 were classified as cyber dependent (ie. an attack on a computer); the rest were fraud. Most reports were from the finance and insurance sectors and were about social media and email hacking. There were 36 reports of ransomware with 13 different strands of the malware identified. Almost 27% of the reports received were from sole traders and micro businesses (less than 10 staff).
- The prohibition of accountancy services in Russia means that the professional bodies are working hard to ensure their members can withdraw their services safely from individuals and businesses with links to the country, where appropriate, following on from recent legislation.

ON THE HORIZON

- Businesses are expected to be targeted by electricity refund scams as the cost-of-living crisis escalates. Individuals are currently being targeted by phishing emails offering refunds for overcharges on electricity bills.

- New research exploring the potential benefits of taking a local public health approach to combatting fraud is due to be published in Q4 this year (funded by the Midlands Fraud Forum and West Midlands Police and Crime Commissioner's Office). Such an approach starts with looking at the needs of a group of people vs. individuals to improve the safety of everyone. Similar approaches have been used for other crimes, including violent crime.
- Reform of Companies House introduces new verification requirements. Companies House will verify UK-based firms; independent verification service providers (such as lawyers and accountants) will verify overseas entities.
- A new Government 10-year fraud strategy is on the way.

COMING UP …

- The Fraud Advisory Panel is hosting a free webinar on practical steps to buying goods and services safely: what to check and how to check it (13 September). Guest speakers are Laugh Hough from BDO's International Institutions and Donor Assurance Group, and Joanna Kozlowska and Christophe Pflieger from BDO's Corporate Intelligence team.
- Our previous webinar on preventing fraud makes good business sense is now available to watch on-demand.
- From 05 September until 30 November the business fraud campaign will focus on how to prevent staff fraud. A supporter's pack and new guidance will be available shortly from website www.lovebusiness-hatefraud.org.uk.

TAKEAWAYS FOR BUSINESS

1. Read the National Cyber Security Centre's guidance on reducing the likelihood of unauthorised movement of business data by malicious insiders. It outlines some technical measures that businesses can implement to prevent this from happening (including monitoring) and explains how to conduct audits following an incident.