Briefing note

The Cost of Living Crisis – Be Fraud Aware

Gillian Baker
Financial Risk Management Lead, Third Party Administration

It's been a turbulent time recently, with high energy prices, high inflation and soaring interest rates resulting in a 'cost of living crisis', related supplier issues and, generally, a flaky UK economy.

Alongside uncertainty, concern, financial pressure and some levels of stress or even panic, there is also an increase in fraud and crime as we perhaps respond to situations differently than we normally would.

The Facts

Citizens Advice reported in June 2022 that more than three quarters of UK adults said they have been targeted by a scammer this year - a 14% increase compared to this time last year.

UK Finance's latest half-year Fraud update, which was published in October 2022, highlights that over £600 million was stolen through fraud and scams in the first half of this year.

The Methods

Social engineering continues to be the main driver leading to fraud losses, with fraudsters using calls, texts, emails, and fake websites all of which are designed to trick people who are feeling a bit vulnerable due to the current economic situation into handing over personal details and passwords.

The Scams

Citizen Advice have reported the following most common types of scams:

- Deliveries, postal or courier services (55%)
- Someone pretending to be from the government or HMRC (41%)
- Someone offering a fake investment or financial 'get rich quick' schemes (29%)
- Rebates and refunds (28%)
- Banking (27%)
- Online shopping (24%)

- Health or medical (13%)
- Energy scams (12%)

With energy scams in particular, Action Fraud reported in September 2022 that more than 1,500 reports had been made to the National Fraud Intelligence Bureau (NFIB) about scam emails offering energy rebates from the regulator Ofgem.

The fraudsters are using the Ofgem logo and colours to make the email appear authentic and provide links for the recipient to follow to apply for the rebate. For those clicking on the links, they are taken to malicious websites designed to steal personal and financial information.

Luckily, savvy members of the public spotted the fraudsters' error – the emails asked for action to be taken before September **2020**, which resulted in many recipients subsequently reporting the scam.

Similar scams are claiming the government is giving £200,000 out at random to people who are of pension age, disabled or on a low income. Sounds feasible that certain groups of society may be entitled to more support from the government but on the other hand, it also sounds too good to be true?

What to tell your members

- Look for errors, typos, poor grammar, or generic salutations like Dear customer rather than a personalised message.
- Consider if the firm contacting you would really be offering "free money"?
- If there are any doubts about the authenticity of a message, contact the organisation directly.
- Don't use the numbers or address in the message – use the details from their official website. Remember, banks (or any other official source) will never ask their customers to supply personal information via email.
- If an email looks suspicious, forward it to Action Fraud using their Suspicious Email Reporting Service (SERS): report@phishing.gov.uk who will investigate and take action if required.
- Action Fraud also note that most phone providers are part of a scheme that allows the reporting of suspicious text messages for free by forwarding it to **7726**. The provider can investigate the origin of the text and, if it's found to be malicious, arrange to block or ban the sender.

In these uncertain times, our money and savings are even more precious to us than before, so it makes sense to stop, think and challenge ourselves before acting on unsolicited emails, texts, or calls. Please share this message with your members.