LIGHTHOUSE FINANCIAL ADVICE

Stay safe - Fighting fraud together

Take a moment to pause and reflect before parting with your money

Question any suspicious motives using our tips in the table below

Stay vigilant and report all suspicions to help keep yourself and others safe

Stay safe - Fighting fraud together

At Quilter we respect your privacy and the confidentiality of your personal data. We want to help ensure that you're doing everything you can to stay safe, especially when dealing with your finances.

Details of the latest scams are reported in the media, daily. There have been cases of fraudsters impersonating financial services companies, including Quilter. They use techniques such as creating bogus websites, sending 'cloned' emails that pretend to be from a real organisation, and most recently we have identified fraudsters attempting to convince clients that a bone fide business has changed its bank account details to encourage funds to be paid into the fraudster's own account.

To become scam-smart and reduce the risk of fraud we urge you to review our up-to-date guidance on how to keep your finances safe by visiting our dedicated Stay Safe page, which includes a scam reporting form if you believe you have been targeted. You can access the page ***here***.

Fraudsters impersonating Quilter, financial services providers and financial advice firms

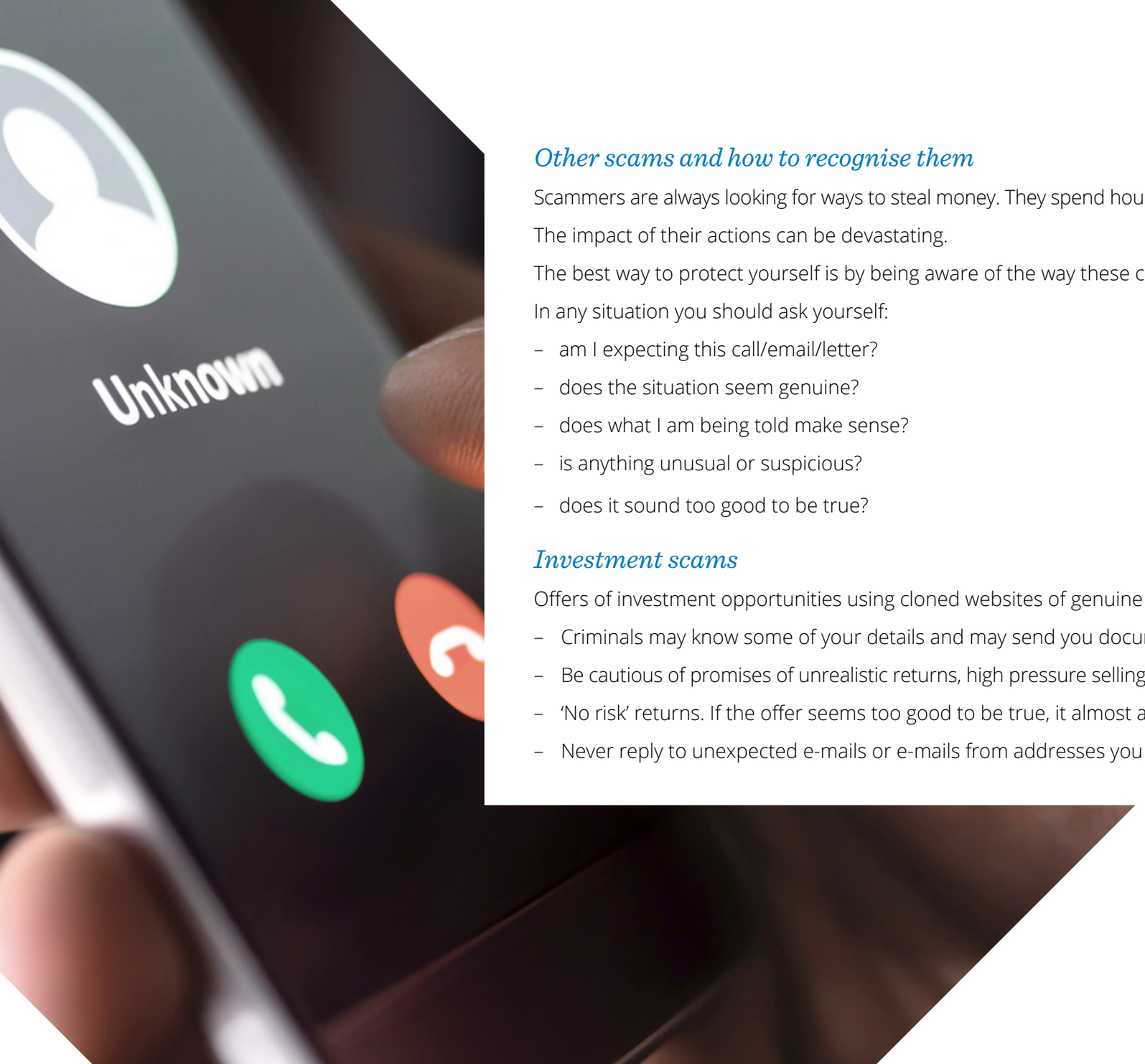
Recently, there has been a rise in the number of fraudsters who set out to impersonate Quilter and other financial services providers. This often involves criminals impersonating a genuine organisation by:

- setting up bogus websites using the firm's name and/or logo. (You can find a list of Quilter's official websites ***here***)
- sending a 'spoofed' email. (You can find a list of Quilter's official email addresses ***here***)
- setting up fraudulent bank accounts

Quilter has been targeted by each of these methods. Fraudsters are often articulate and knowledgeable, using sophisticated techniques to impersonate companies and research their targets, making their scams look like genuine investments. Typically, experienced investors and those over 65 with savings in excess of £10,000 are targets for investment fraud - but anyone can be a target.

The only way to protect you and those dearest to you is by being aware of the ways these crimes are committed so you can be one step ahead.

Continued overleaf



Other scams and how to recognise them

Scammers are always looking for ways to steal money. They spend hours researching to find information they can use to gain your trust.

The impact of their actions can be devastating.

The best way to protect yourself is by being aware of the way these crimes are committed so you can be one step ahead.

In any situation you should ask yourself:

- am I expecting this call/email/letter?
- does the situation seem genuine?
- does what I am being told make sense?
- is anything unusual or suspicious?
- does it sound too good to be true?

Investment scams

Offers of investment opportunities using cloned websites of genuine investment providers.

- Criminals may know some of your details and may send you documentation and links to websites that appear genuine
- Be cautious of promises of unrealistic returns, high pressure selling, and offers that are dependent on time limited decisions to buy
- 'No risk' returns. If the offer seems too good to be true, it almost always is
- Never reply to unexpected e-mails or e-mails from addresses you don't recognise

Continued overleaf

Cash machine fraud

What you should look out for.

- Does the cashpoint look as it should? Has it been tampered with?
- Protect your pin to avoid it being seen
- If your card is retained by a cash machine report it to your bank immediately
- Limiting the amount that can be withdrawn daily from your account
- Destroy any cash machine slips safely
- Report any concerns to your bank immediately

Impersonation fraud

Your personal information is stolen and used to open bank accounts/apply for credit cards/Government benefits/ loans/driving licenses/passports for example.

- Protect your privacy – be careful what information you put on Social Media
- Cross-shredding device to dispose of personal data e.g. bank statements, items containing personal information
- Never share passwords
- Never give information to verify your identity unless you are sure of who you are in contact with
- Never reply to e-mails requesting personal information – verify the authenticity of the e-mail independently
- Check your credit report regularly for rogue accounts
- Be aware contact can come from Criminals posing as different types of organisations including HMRC, NHS, Banks etc
- Be cautious of requests that require you to provide information immediately to avoid being penalised

Continued overleaf

Phone/cold calling scams

Fraudsters often contact people by phone posing as their bank, HMRC or another trusted source.

- They will try to obtain personal information by posing as a legitimate/trusted enterprise
- They may 'spoof' the number that they use to call victims from to make the request appear genuine
- Never give your personal information over the phone

Invoice scam

Criminals pose as someone from an organisation you trust and provide you with new or amended bank account details.

- If you receive a request for funds check the contact details and account numbers independently
- Ring the company concerned to verify the request

Remember - STOP! CHALLENGE! PROTECT!

Scams are a crime. Don't be embarrassed to ask for support from those you know and trust. Where you are suspicious of activity it's important to report it immediately.

Continued overleaf

Who do you report suspected fraud to?

Quilter

If you believe you've been targeted by online scammers who are impersonating any of Quilter's brands or financial advice firms, please complete this form.

https://www.quilter.com/scam-report-form

Action Fraud

National reporting centre for fraud and internet crime. Call the helpline for advice on preventing fraud and what to do if you fall victim to it or use the online fraud reporting service.

Tel: 0300 123 2040 Textphone: 0300 123 2050 ***www.actionfraud.police.uk***

Credit Industry Fraud Avoidance Scheme (CIFAS)

Fraud prevention organisation that provides a protective registration service to protect people whose details have been stolen.

http://www.cifas.org.uk

Citizens Advice

National network of free advice centres offering free, confidential, and independent advice, face-to-face or by telephone.

England: 0800 144 8848

Scotland: 0131 550 1000

Wales: 0800 702 2020

https://www.citizensadvice.org.uk

Your Bank

If you have made a payment and believe the request was a scam, contact your bank immediately. They may be able to recover some of your money.

If you or someone else is in immediate danger because of a scam (for example, if you are being threatened by an aggressive doorstep caller), call the police on 999 or 112.

Take Five is a campaign offering straight-forward and impartial advice to help everyone protect themselves from financial fraud.

http://www.takefive-stopfraud.org.uk