



PROTECTING YOURSELF FROM FRAUD

Client information

Protecting Yourself from Fraud

2plan understands that with the advent of AI and data leaks, criminals have become more and more savvy when it comes to Fraud.

We want to help protect you from the increasing threat of fraud and investment scams, by firstly explaining how we contact you and what we will and won't ask you; and how you can do things to make sure your money and personal information stays in your hands!

Investment scams are becoming common and this guidance documents common techniques used by criminals when trying to get potential victims' information or to invest in a scam investment.

Investment Scams

Unless you advise us otherwise, we will communicate with you via one or more of the following methods: face to face, email, secure website, SMS, telephone and letter.

Over the phone

In the most common scams, fraudsters will call their victims often impersonating a legitimate company or financial adviser.

One of the things our clients like about 2plan, is that it will mainly be **your adviser** who contacts you; however, there are some instances where a member of the team will contact you instead.

As a business we will always verify you through our security questions and we will never ask for details such as your National Insurance Number, full Account numbers, full date of birth or other such sensitive information.

Should you not be comfortable on a call, hang up, and call our number to verify if the call was indeed legitimate. Please contact admin@2plan.com or call us on 0113 302 1360 (9am – 5pm, Monday to Friday).

In person

We will never come to you unannounced, and most certainly not with someone you are not familiar with.

2plan advisers will always ensure that meetings are prearranged, usually taking place at our offices or another location at your request.

Contact by Post or Email

From time to time, you will receive financial promotions from us, these will usually be tailored to you, they will be clear and balanced and will never guarantee any kind of performance promises.

We will also always ask you to contact us if you are interested.

If you receive any unexpected or unusual correspondence from your adviser, contact them using the phone number you would usually use (rather than any numbers in the correspondence) to confirm that they have in fact sent the communication, do not respond or provide any personal information until you are certain that the communication is genuine and do not click on any links that may have been sent via email.

If you are concerned about a communication, you have received regarding 2plan products and services, please contact your Financial Adviser directly.

Alternatively, please contact admin@2plan.com or call us on 0113 302 1360 (9am – 5pm, Monday to Friday).

Documents and investments

Scammers will attempt to form a friendly relationship and build trust before asking you to invest. The documentation they present will appear to come from a regulated firm that you can find on the Financial Conduct Authority (FCA) register. Usually, they will offer investments in emerging, unregulated markets or property.

Fraudsters will promise much higher returns than that of established investments however the investment does not exist or has no value. They will likely push you to invest there and then.

2plan advisers will follow our advice process which will include a thorough fact find of your circumstances and your specific objectives. We take the time to ensure that all our product recommendations and services that we provide deliver the best possible outcomes for all our clients, therefore on we will **always** have more than one meeting.

The first will be the **consultation** meeting where we will get to know you, your financial objectives and goals, financial priorities and timelines.

Where we are considering your investment needs, we will assess your attitude to investment risk and capacity for loss, this will help us to understand how much risk you are willing to take with your capital.

We will then have a second meeting where the **Advice** would be presented and any advice provided will be confirmed to you in writing. We would not request that you sign up there and then.

What can you do to protect yourself from Scammers?

The Individuals who are approached to invest in scam investments are often as a result of their personal data having been compromised. Below are some practical ways to keep your information secure and avoid becoming a victim:

- **Use different passwords for different websites and update them regularly.**
- **Use a combination of letters, numbers and other characters where possible.**
- **Do not publish any personal information on social media that could be used by a criminal to commit fraud.**
- **Monitor your bank statements regularly and notify your bank as soon as possible if you notice anything suspicious.**

Fraudsters will look to gain access to you in many ways; here again, are some things to look out for:

- **Unsolicited phone calls, text messages or emails.**
- **Not completing a security process or asking for personal data as questions.**
- **Pressure to make a quick decision.**
- **Contact details that are only mobile phone numbers or PO Box addresses.**
- **Offer of an unusually high return on your investment for very low risk or guarantee a certain return.**

What should you do if you receive unsolicited contact about an investment?

Always contact your adviser before you invest to confirm the legitimacy of the person you have been speaking to and if you are still unsure, check the warning list the [Financial Conduct Authority \(FCA\)](#) publish to see if they are aware if the firm has been impersonated. Don't just rely on [Companies House](#) data.

If you have previously been a victim of fraud, you are also more likely to be targeted for further frauds and scams; it is important to remain vigilant and make sure that your passwords have been changed.

What to do if you become a victim of fraud?

If you find that you have become a victim of fraud, we recommend that you report this to law enforcement by making a report to [action fraud](#).

You should also inform your bank and any other financial institution you hold accounts with.

If you believe that your personal data has been compromised, we recommend signing up with a credit referencing agency so that you can monitor your credit file for any accounts that have been set up without your knowledge. You may also wish to apply for a protective marker to be placed against your name and address; this can be applied by contacting [CIFAS](#). The protective marker will alert credit reference agencies that you have been a victim of fraud and prompt them to conduct extra checks on any applications they receive to ensure it is you they are dealing with.

If you have been a victim of Investment fraud, be wary of companies claiming they can recover money from lost investments on your behalf for a 'one-off' fee. This could be the same fraudsters trying to scam you again.

Further Information

We have provided links to a number of websites below, dedicated to helping keep you and your personal information safe online.

Please note, we accept no responsibility or liability for the content or availability of any external site.

[FCA Warning List](#) – This provides details of any firms that are being targeted by scammers.

[Take Five](#) – Practical advice on how to protect yourself from fraud.

[Action Fraud](#) – National Fraud and Cyber Crime Reporting.

[Bank Safe Online](#) - Helpful tips & advice to safely bank.

[Get Safe Online](#) – General Advice on how to stay safe online.

[CIFAS protective registration](#) – Fraud Protection Register.