Quilter

Fighting impersonation fraud – how to spot a criminal posing as your client

Help protect your client from being a victim of fraud. Learn the red flags for impersonation fraud and prevent criminals from getting access to your clients' funds.

£12billion
stolen by fraudsters in 2022

207,372
impersonation scams (authorised push payment fraud) reported in 2022

Did you know?

In 2022 there were 207,372 impersonation scams (authorised push payment fraud) reported, up 6% on the previous year contributing to a staggering total of over £1.2 billion stolen by fraudsters.

Source: https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023

How does impersonation fraud work?

1

The fraudster hacks into your client's email account and accesses information about their investments and their relationship with you from their sent items.

2

Posing as your client, they will send an email to you requesting an urgent withdrawal of their funds. They will ask that these funds are paid to a bank account that's different from the usual (which the fraudster controls) and will ask you not to call them to discuss over the phone. Often with an elaborate story as an explanation.

3

They are likely to provide a copy of a bank statement to verify the details of their 'new' bank account. They will send these documents to you for certification.

4

The fraudster will monitor the email account and intercept any emails from you before your client sees them. When processed, the fraudster will receive the funds in the new account before the client is aware of the activity. But by then, it's too late.

** Figures from UK Finance*

For financial advisers only

Don't get caught out –

an example of impersonation fraud in action

Adviser A received an email from a long-term client asking to withdraw a large sum from their investment. The client's email mentioned that they were feeling very unwell and were unable to speak over the phone. The email was shorter than usual and didn't have the same friendly tone that the client normally used – but Adviser A thought perhaps that was because they were feeling ill.

Adviser A also noticed that their client had asked for the payment to be made to new bank account details. They emailed their client asking them to provide a copy of a statement showing the new details which the client sent electronically, along with a message that insisted they needed the money urgently.

The more Adviser A thought about it, the more the situation seemed strange. Why would their client want to withdraw from their investment now, years before they'd planned to? What was so urgent? Despite their emails, Adviser A decided to call their client using the contact number on file, just to be sure. When they spoke over the phone, Adviser A found that their client wasn't ill at all and in fact their email account had been hacked by a fraudster.

A simple phone call from Adviser A had prevented their client's money from being stolen by a criminal.

Raising the red flag for impersonation fraud

Before processing any email instructions, ask yourself the following questions:

1. Does the email contain uncharacteristic poor spelling, grammar and/or a mix of upper and lower case letters, or just not make sense? Yes ☐ No ☐
2. Is the tone of the email different to what you'd expect from this client? Have they used an unusual greeting? Yes ☐ No ☐
3. Does the request to withdraw funds contradict their agreed investment strategies? Yes ☐ No ☐
4. Has your client asked you not to call them, perhaps giving a reason like feeling ill, attending a family funeral or being abroad? Yes ☐ No ☐
5. Are the funds to be paid to a bank account that's different from the usual? Yes ☐ No ☐
6. Does the withdrawal request exceed the current policy amount? Yes ☐ No ☐

If you answer 'Yes' to any of the above questions, this is a red flag for potential fraud and you should call your client on a telephone number you know to be theirs to confirm the request is legitimate. Just a quick call could prevent serious emotional and financial stress for both you and your client.

Protecting your clients from impersonation fraud

We have robust processes and controls in place to help prevent impersonation fraud, and will always investigate any transactions we feel could be suspicious.

As their financial adviser, you can demonstrate the value of your service to your clients by doing all you can to keep their money safe from criminals. Being aware of the ways a fraudster could try to steal your clients' money demonstrates best practice and could prevent the upset and worry your client could experience as a victim of impersonation fraud, as well as ensuring there are no financial or reputational consequences for your firm.

quilter.com

QIP 23018/59/4591/October 2023