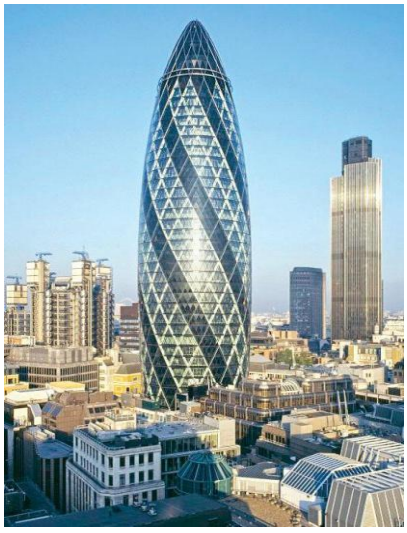
HINDSIGHT

Collegiate Underwriting

CLAIM ALERT **January 2016**



Welcome to the latest edition of our Hindsight publication.

We have recently seen a spate of email hacking frauds against clients of IFA's where the fraudsters have duped the IFA into encashing investments and forwarding the proceeds to bogus bank accounts. Some of these have involved thefts of sums greater than £100,000. You can well imagine that it is incredibly distressing to clients to discover that substantial amounts of their life savings have been stolen and it is exceedingly unpleasant for the insured firm to realise they have been duped and find their own procedures coming under scrutiny and having to accept that with a little more care the theft could have been prevented.

The fraudsters have considerably upped their game and no longer can they be relied upon to send fake client emails with ludicrously poor grammar making them easy to spot. As the client's email account has been hacked, the emails come from the actual client's email address. The fraudster will often have been able to review previous email exchanges between the firm and their client so they can mimic the clients writing style and develop the conversation seamlessly from the previous correspondence. There is no reason for the IFA to suspect that they are not corresponding with their client.

A typical approach would be to ask for an updated portfolio valuation because they are considering a possible property purchase. The IFA replies with the valuation, which is seen by the fraudsters, but deleted from the clients hacked email account so the client is not aware of the exchange. This is easy to do as the fraudster sets the client email account to forward all emails from the IFA to another email account and then automatically delete it from the clients email account. A little later the fraudster will follow up the earlier email, enquiring what the penalties would be for encashing say £100,000 and whether there would be any tax consequences. Again the reply is deleted before the client sees it and they remain in the dark that their savings are under imminent threat. Then comes the email requesting £100,000 to be transferred into a bank account giving the clients name but a different sort code and account number to what the IFA has previously used. That email often may also state the client is currently travelling so will not be contactable by phone. They are then only a forged signature on a scanned withdrawal away from hitting the jackpot.

As we have said the fraudsters are sophisticated and in some cases have set up fake email accounts so they can email the client and pretend to be the IFA firms in order to cancel meetings etc. so that the client remains in blissful ignorance until it is too late.

We would strongly urge you to review your current procedures and consider whether your firm would be similarly duped.

Unfortunately many banks seem to think it is acceptable not to check account payee names actually match account numbers and sort codes or seem to be fairly vulnerable to opening accounts up on the basis of faked ID. Clearly there is a debate to be had as to where responsibility lies between the client for having his email account

hacked, the bank for their general sloppiness and the firm for not spotting they were being duped. That is for another day, the purpose of this email is just to highlight this is a growing risk and you need to think carefully as to what checks and balances you can introduce, to protect your clients and hence yourselves from this growing area of Fraud.

Hindsight Claim Alert — January 2016

Questions to consider;

- **Are your advisers and account administrators aware that just because an email comes from the client's known email address it doesn't mean it has actually been sent by the client**
- **If they got a large withdrawal request would it occur to them to review the client's advice file to see whether that was consistent with the clients previously recorded strategy?**
- **Would they always double check that account details provided matched the client's known previous account details. If they were different are they aware that any verification information supplied by email to support the new account could be quite easily forged.**
- **Would they process a large encashment without actually speaking to the client, particularly if there is an urgent deadline and the client was out of mobile signal?**
- **Even if the "client" called them, would they recognise their voice or have security questions that could be asked that would not be readily knowable from information in the hacked email account?**

Please accept my apologies for starting 2016 on such a negative note but given the alarming increase in claims of this nature we though it important to get the message out as soon as possible.

My thanks go to Martin Archer, our Legal Director, for producing this newsletter.

We hope that you find the content informative and useful. If you have any comments on the content, or suggestions for future issues, please write to us or e-mail on newsteltter@collegiate.co.uk

Richard Turnbull
Underwriting Director
Collegiate Underwriting

Collegiate Underwriting is a trading name of
Collegiate Management Services Limited
Registered Office:
Mint House
18 Mansell Street, London E1 8FE

Telephone: 020 7459 3456
Facsimile: 020 7459 3455
E-mail: cms@collegiate.co.uk
www.collegiate.co.uk
Registered in England No. 02065041

Collegiate UNDERWRITING