National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Client Impersonation Fraud

January 2016

CLIENT IMPERSONATION FRAUD

The information contained within this alert is based on the result of engagement with industry and research carried out by the National Fraud Intelligence Bureau (NFIB). One of the key objectives of sharing fraud data between the NFIB and the Financial Services Industry is to prevent fraud. The purpose of this alert is to inform the industry of a fraud some of your Independent Financial Advisors (IFA) members have very recently been targeted by, and to provide suggested measures to prevent further instances of fraud.

ALERT CONTENT

Fraudsters are targeting Independent Financial Advisors (IFAs) by impersonating their clients in order to request that funds be removed from an investment product and paid into an account (or accounts) controlled by the fraudsters. These instructions appear to have been sent from the genuine client's email address, which may have been hacked, or 'spoofed' by the fraudsters. If the initial request is successful, the suspects have been known to attempt additional transfers, often to a number of different accounts.

The fraud is successful because the instruction appears to originate from a genuine client, and a lack of secondary controls employed by the IFA prior to acting upon the request.

PROTECTION / PREVENTION ADVICE

Before acting upon instructions received via any means, consider the following:

- Verify the source of the instruction by using another, well-established means of contacting your client; preferably via phone. Do not use contact numbers included on or with the instruction.
- Be aware that the fraudsters may also have cloned, or 'split' your client's SIM card, or arranged for their phone line to be redirected. As such, ask additional security questions that would only be known to the client. Consider what questions would be suitable – if your client's email has been hacked, what other information is and is not likely to be available to the fraudsters?
- Consider the tone, spelling, time of day and format of the email and/or the instruction. Is this consistent with your existing relationship with the client?
- Be extra cautious whenever one instruction is followed up in quick succession with another; particularly when the client is asking for funds to be paid to multiple accounts that you have not previously paid out to.
- If you have acted upon an instruction subsequently found to be fraudulent, contact the recipient bank immediately.

If you receive a fraudulent request from someone purporting to be your client, report this to Action Fraud on 0300 123 2040, or via http://www.actionfraud.police.uk/report_fraud - regardless of whether have you acted upon the instruction or not.

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete.

If you have other feedback or additional information that you would prefer to provide by email please send to NFIBfeedback@cityoflondon.pnn.police.uk.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**PROTECT**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	V1.0
Storage File Location:	G:/OPERATIONAL/Fraud_Intel/Intelligence
Purpose:	Fraud Alert
Owner:	NFIB Management
Author:	96583, Senior Analyst / crime reviewer
Review By:	96583, Senior Analyst

Practical Guidance for PROTECT documents

This document is classified **PROTECT**. In government and law enforcement this determines the security measures that are required to protect it. This means:

- Only permit members of your staff who have a genuine 'Need to Know' to see the contents of the document;
- Do not copy the document or any of its pages without written approval of the Director of Intelligence NFIB;
- Do not pass on the document, or disclose any information contained in it, to any third party (outside of your business) without written approval of the Director of Intelligence NFIB;
- Do not read or work on this document in public areas;
- Lock the document in a secure cabinet when it is not being used; and,
- Only dispose of this product by shredding, pulping or incineration.