



AUM Law primarily serves the asset management sector, with specific expertise in the regulatory space. We focus on providing truly practical, forward-thinking advice and services.

This bulletin is an overview only and it does not constitute legal advice. It is not intended to be a complete statement of the law or an opinion on any matter. No one should act upon the information in this document without a thorough examination of the law as applied to the facts of a specific situation.

Please contact [a member of our Regulatory Compliance Group](#) to ask a question, submit a comment or request more information about any topic in this bulletin. To unsubscribe or request a copy of one of our other recent bulletins, please contact communications@aumlaw.com.

The following is a warning for all firms about a frequent scam we have seen perpetrated in the securities industry over the past number of years. We want to take this opportunity to warn everyone to be wary any time a client asks you to transfer their assets to a bank account that you were not previously made aware of.

The Scheme in a Nutshell

The firm will receive an email from their “client” asking to redeem a portion of their assets and ask that the money be transferred to a bank account that is not on file. The request will usually come from the client’s email account at a time when the client is out of town or otherwise unable to access their email for a period of time.

The email requesting the money transfer is sent to the firm as part of a chain of previous correspondence between the actual client and the firm, and includes a signed redemption request to the new bank account. The signature on the request matches the actual client’s signature on file. From that point, the firm and the fake “client” will correspond several more times about a variety of topics, and leaves the firm with the impression that the redemption request is legitimate.

This scheme is particularly disconcerting as the fraudster demonstrates an unusually high level of knowledge about the client’s personal information and is able to use that information to give the firm comfort through email that there is no fraudulent activity involved.

Similar Frauds in the Industry

While this was the most sophisticated version of the scheme that we have seen, it is not uncommon that we have heard stories about a hacker entering a client’s email account and requesting a redemption of funds to a new bank account. It is very important to ensure your firm maintains up-to-date security for your computer systems, including email, and keep in mind that your clients’ email accounts may also be potentially vulnerable to outside parties.

How to Protect against Similar Fraudulent Transactions

In order to protect your firm and your clients against similar fraudulent activity, we recommend that you implement specific procedures in relation to redemption requests for new bank accounts. Firms should always be wary whenever a client makes a request for funds to be transferred to a previously undisclosed bank account. Some procedures you may wish to consider to minimize the risk include but are not limited to, the following:

- call the telephone number on the client’s file to confirm the request;
- require you meet the client in person to confirm the request; and/or
- transfer funds only to accounts on file.

FINTRAC Reporting Requirements

Please be advised that once you have reasonable grounds to suspect an actual or attempted fraudulent transaction is related to money laundering or terrorist financing, you are required to submit a suspicious transaction report with FINTRAC within 30 days. If you do not believe it is related to either activity, we still strongly encourage you to contact your local police department and the RCMP to report the identity such fraudulent transactions.

For more information on the FINTRAC reporting requirements, please visit <http://www.fintrac-canafe.gc.ca/publications/brochure/05-2003/2-eng.asp>.

If you have any questions or would like to discuss further, please contact any member of our [Regulatory Compliance group](#).