Growing Hazard for RIAs: Sophisticated Email Fraud Attempts

By Rita Dew, Founder and President, National Compliance Services

Internet criminals have become highly sophisticated in recent years, and many can hack email address books with ease. Some are using that capability to target unwary advisors with emails purporting to be from their clients, requesting that funds be transferred to them immediately for an urgent purpose.

If you are caught off guard by a criminal and transfer funds as requested, guess who’s left holding the bag? In most cases it’s you, of course. But even paying the price may not leave a client content with that resolution. You would not want to put a client through the disruption involved in setting things right, and possibly causing that client to question your quality control procedures and your judgment.

The U.S. Treasury Department’s Financial Crimes Enforcement Network reports that such cases in the financial services industry have grown by 1,000% over the last decade. Nearly 4,000 incidents occurred last year, according to the agency. And a survey by the National Cyber-Forensics and Training Alliance found the majority (62%) of email-based wire fraud attempts were trying to move funds to domestic banks. A domestic bank might arouse less suspicion from advisers than a foreign one, leading to a successful theft.

You can take steps to avoid having that happen—or at least protect yourself financially and legally should it come to pass despite your best efforts to prevent it.
How Fraud is Perpetrated

Even when your clients pay attention to the security of their email accounts, often they and some email service providers are no match for sophisticated hackers. These high-tech burglars can breach security roadblocks, download address books and browse through emails your clients have sent to you and anyone else. Their purpose is to learn enough about your clients to enhance their ability to deceive you by referencing facts or inventing plausible stories (e.g., travel plans) that clients would convey to you, and bait the trap.

That’s what happened last year to Wellesley, Mass.-based GW & Wade, LLC. As of April 2013, the firm had approximately 1,600 clients and $3.8 billion in assets under management—some discretionary, some not. Details of the episode, described in detail in an administrative proceeding before the Securities and Exchange Commission, offer a blueprint of what to do, and not do, to avoid this hazard.

The SEC brought charges against GW & Wade involving its recordkeeping and asset custody procedures. In October 2013, the matter was settled when the registered investment adviser (“RIA”) consented to the SEC’s censure and its “cease and desist” order, along with a $250,000 penalty. Some $290,000 of a client’s cash had been wired to the client’s electronic impersonator in three separate transactions. The RIA had already reimbursed the client for the loss prior to its settlement with the SEC.

“Real Life” Guidelines for RIAs

GW & Wade’s procedural deficiencies, as enumerated in the SEC’s order (Administrative Proceeding File No. 3-15589) include the following. GW & Wade:

• Had custody of certain client assets that it could access and transfer to third parties, but it failed to obtain an examination of those assets by an independent public accountant and to disclose those assets in its public disclosures,
• Had not adopted policies and procedures reasonably designed to prevent violations of the securities laws and rules governing custody of client assets,
• Failed to maintain required records for certain custodied accounts, and
• Did not adequately implement its policies and procedures for calculating its advisory fees in discretionary accounts, which resulted in billing overcharges to certain clients.
The practice that may have contributed most to the fraud was GW & Wade’s maintenance of letters of authorization (LOA) “signed by some clients but otherwise left blank for over 900 accounts,” according to the SEC. When a client requested a transfer of funds and a duly validated LOA was not in place, the RIA would simply fill out the form. “The practice enabled GW & Wade to transfer client funds without having to obtain client signatures in every instance,” the order states.

Also, the firm’s adviser representatives “on occasion” simply cut out a client signature from previously executed (but expired) LOAs, and pasted them into a new LOA upon receiving a client wire transfer request.

**Classic Tactics**

The fraud perpetrator’s tactics were classic: Each email requesting that funds be transferred to a foreign bank stated that the emailer could not get to a telephone due to being in the middle of a meeting or at a funeral, but needed the funds to be disbursed that day. “Because GW & Wade maintained pre-signed LOAs and did not have any procedures in place to confirm the authenticity of wire requests made by email, the client’s funds were wired without the client’s knowledge or authorization,” the SEC stated.

Prior to its settlement with the SEC, GW & Wade promulgated several procedural changes to limit its exposure to this type of fraud going forward. Those steps included:

- Implementing a wire transfers, checks, and journal disbursements policy eliminating the use of pre-signed LOAs and requiring advisors to confirm transfer requests by telephone,
- Putting in place an account management system under which access to most client accounts will be read-only, and
- Instituting policies and procedures for tracking and safeguarding password and log-in information for outside client accounts and for maintaining appropriate books and records of all transactions in custodied outside accounts, regardless of whether GW & Wade conducts transactions in those accounts. (See accompanying tips on password best practices.)

Another basic policy you might want to adopt is a dollar limit on all wire transfers.

**Pointers for Strong Password Protection**

You have probably heard most of these admonitions before, but a review of password integrity best practices is a good idea. Here are some basics:

- Never use potentially familiar personal information in a password,
- Do not use the same password for multiple accounts,
- Avoid passwords that are similar to your user name,
- Use passwords that combine letters, numbers and symbols,
- Change your passwords on a regular basis, and
- Avoid sharing your passwords with anyone, and when sharing is essential, never do so via email.
As part of the settlement, GW & Wade was ordered to retain an independent consultant for a two-year period to perform a comprehensive review of the firm's written policies and compliance procedures “reasonably designed to ensure that it is meeting its custody and related books and records obligations.”

**Signs of Trouble**

Even if your policies and procedures already meet the standards the SEC enumerated for GW & Wade, it is helpful for you and your staff to be made aware of the signs of an email fraud attempt. These include:

- Spelling and grammar in the fraudulent emails is often poor,
- There is occasionally an indication the funds transfer is urgent,
- Wire requests may be international, but domestic request are on the rise
- Perpetrators generally prefer to only communicate by email, occasionally claiming they do not have access to a phone or visit in person, and
- There may be indications that a client’s signature has been copied. Watch for faint or misaligned signature lines.

The sidebar below illustrates some of these red flags.

**Urgent Appeal for Cash: An Eye for an “I”**

The following is an illustrative example of an email sent on Thanksgiving Day from a client imposter to an adviser. Some of the telltale signs of fraud are evident. One essential ingredient—a false email address for the adviser to use to maintain the dialog with the alleged client—was particularly subtle, requiring sharp eyes to detect. The phony email address substituted an “l” for an “i.”

**Sent:** Thursday, November 28, 2013 11:53 AM  
**Subject:** Very Urgent

*It takes me great pain to write this but I need your help.  Few days back we made an unannounced vacation trip to Manila, Philippines. Everything was going fine until last night when we got mugged on our way back to the hotel, all cash and credit card were stolen off us but luckily for us we still have our passports with us. I’ve been to the Embassy and the Police here but they’re not helping issues at all they asked us to wait for 3 weeks but we can’t wait till then and our flight leaves in 18 hours from now but we’re having problems settling the hotel bills and the idiot manager won't let us leave until we settle the hotel bills, we are freaked out at the moment …It has really been embarrassing for me... $2000 will cover all my expenses but I will appreciate whatsoever you can afford to wire right now, I promise to refund it to you as soon as I arrive home. You can wire it to my name from a western union outlet around. Here are the details you need to get it to me;*  

[Your] Full Name.  Location - Evangelista Street  
1640 Rudex Building, Makati, 1234, Philippines.  

*Get back to me with the western union confirmation details.*
Even if you establish a requirement that a client be reached by telephone, there is the potential for being deceived. For example, Andy Fotopulos, a senior vice president of the Starkweather & Shepley insurance brokerage firm, recently learned of a case in which the hacker found a way to divert calls to the client’s cell phone to the hacker’s phone. Yet the display on the adviser representative’s phone appears as the “correct” number.

In this scenario, you might think you are leaving a message telling the actual client to call you back if she hadn’t authorized the wire transfer request. Since the true client would never have actually received that message, no such call would be returned. This underscores the need to speak live to the client under all circumstances.

Bottom line: Never get caught up in the heat of a supposedly urgent request. Instead, take a deep breath and ask yourself whether the transaction makes sense based on what you know about the client. Implement rigorous policies and procedures to make sure no one can access client funds without the authority to do so, either directly or through a third party. Also, take the time to receive formal guidance on fraud prevention, and have members of your staff, including your chief compliance officer and chief technology officer, undergo similar training.

**Insurance Protection for RIA Wire Fraud Victims**

E&O and D&O liability coverage and fidelity bonds can afford you some financial protection, particularly when you have already established procedural safeguards that are violated by someone on your team. But do not assume you are already covered for this kind of hazard under your existing policies.

Insurance companies that have ventured into this specialized area of risk include Hanover, Great American and The Hartford. Each has different provisions and limitations, according to Mr. Fotopulos.

Annual premiums for such policies can range from several hundred dollars to multiple thousands, depending on coverage levels, deductibles, the size of your firm and other risk factors assessed by the carriers.

Applications for such coverage, predictably, are very detailed. It will likely be readily apparent whether you will be offered coverage, or offered it at a price you can afford, based on the questions. Beyond the most basic, categories of questions may include:

- Audit and internal control procedures,
- Pre-employment personnel screening procedures,
- Outsourcing of certain services, including payroll management, and
- Prior run-ins with the SEC or state regulatory agencies.

Whether or not you decide to purchase such coverage, it may be advisable to seek quotes for coverage just to determine its cost and availability.
About the Author

Rita G. Dew, Esq. is the founder and president of NCS. Rita is also the managing partner of the law offices of Rita G. Dew, P.A. The focus of her legal practice is on investment management and representing investment advisers and broker-dealer on issues dealing with corporate and securities law in the financial markets.

Disclosures

This white paper is general in nature, and it should not be construed as legal, compliance, or regulatory advice. National Compliance Services, Inc. is not engaged in the practice of law. Always consult an attorney or tax professional regarding your specific legal or tax situation.