BNY MELLON | PERSHING

Fraud-proofing your business

FRAUD IS SURGING. HERE'S HOW TO PROTECT YOUR CLIENTS AND YOUR BUSINESS

Most advisors think they can see through a fraud attempt, but this is becoming increasingly challenging. Fraudsters continue to find new ways to prey on investors and their advisors. Forget the stereotypical image of hackers working out of basements; many are part of large, well-structured criminal enterprises.

As fraudsters become more sophisticated, they're also more convincing. In some cases, advisors are being tricked by fraudsters posing as clients, using actual details from their lives to sell their deception. Advisors without proper safeguards in place can become targets and subject their business, and their clients, to risk.

Consider fraudsters' success rates in recent years. Five years ago, 10% of reports turned out to be real instances of fraud, according to Rob Hulstedt, Vice President at BNY Mellon's Pershing. Last year that number jumped to 14%. To put this in context, the FTC's Consumer Sentinel Network reported that consumers lost $1.48 billion to fraud complaints in 2018 – a 265% increase over the $406 million they lost in 2017.[1]

In large part, that's because fraud scams have evolved and multiplied. Phishing emails about get-rich-quick schemes and robocalls telling investors they owe hundreds of thousands of dollars to the IRS are just the most obvious, entry-level scams. More sophisticated operations, which in some instances may include technology and linguistic experts, and even attorneys, are highly systematic and focus on how and where they can have the most impact. In other words, fraudsters have become expert impersonators.

It's one thing to fall for a scam when it's your money, but stakes are even higher when you're responsible for someone else's wealth. Having to restore lost funds could put your finances in jeopardy, while the potential reputational damage may jeopardize your client relationships.

While fraudsters are more skilled today, succumbing to them isn't inevitable. By understanding the nature of cyber-fraud in 2020 and how it's likely to change in the coming years, you can develop a plan to keep your clients' assets and your business safe.

Knowing what you don't know

Effective fraud preparedness hinges on an advisor's (and the institution's) attitude towards preparation. At a firm level, it's not enough to design and implement a cybersecurity and fraud training module and then reuse it year after year. Savvy advisors safeguard their clients' assets and their reputations by avoiding complacency and acknowledging what they don't know. The fraud landscape is ever-changing, so ongoing training – with frequently updated modules and an emphasis on best practices – is a must.

For example, at many firms, it's not uncommon for advisors to focus only on the routing and account numbers on incoming wire requests. If those two numbers match what's on record for the client, the request will usually be fulfilled. The problem is that the numbers do match on many fraudulent requests, but deeper digging reveals that the name does not. In essence, what might appear to be a first-party request (usually considered fail-proof) is actually a third-party transaction. In this case, failing to address that detail opens an advisor and the firm to significant risk.

Typically, these steps aren't skipped out of carelessness on the advisor's part. More likely, they're trying to respect the client's time, especially when nothing else appears out of place. For instance, one might not be inclined to verify that a disbursement request is real if it fits with a long-time client's familiar habits and behavioral patterns. Alternately, when an advisor already knows the client has a project on the go, such as a renovation or a real estate purchase in the works that requires a transfer of funds, this may not trigger the need for additional diligence.

But the idea that fraudulent communications will always be easily identified – either because they're riddled with grammar and spelling mistakes or contain inadequate or inaccurate identifying information – is wrong.

Fraudsters use proofreaders and have perfected the art of email hacking. As a result, they often have access to a wealth of personal information – including passwords, account numbers and knowledge of significant life events and recent transactions. And even if you know your client's voice and mannerisms well, your colleagues – who might be on the receiving end of a fraudulent request delivered over the phone – probably don't.

The gold standard of fraud detection

Apart from ensuring anti-virus/malware software and firewalls are installed and up to date, preventing fraud doesn't require special tools or technology. What it does require is a consistent focus on the potential for security breaches and how to identify them accurately. In other words, a proactive mindset and a handful of simple behaviors will protect your clients and your business from attack.

Common sense and a simple phone call are the gold standards for fraud detection. All wire transfer requests an advisor receives, even if they look legitimate, merit a follow-up phone call on the investor's phone number of record.

Is the request consistent with past activity? Has the client already told you he was thinking about renovating and now he's emailing with a contractor's invoice and a disbursement request? When in doubt, make the phone call. Four out of five fraud attempts are stopped this way, says Hulstedt.

Additional measures like verbal passwords are helpful, too. Sometimes you won't reach the client right away, and that's okay. A good best practice here is to wait until you can. Most legitimate requests won't have the same urgency as a fraudulent one, and if the client does express irritation at having to wait, explaining that it's for security reasons will mitigate it. The same goes for last-minute requests to call the client at a different number – a big red flag. Without exception, always call the client on the established phone number of record.

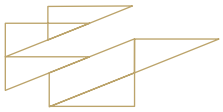
Of course, understanding the importance of the follow-up phone call, in theory, doesn't guarantee you'll remember to use it in practice. Both investors and advisors need regular opportunities to reinforce their knowledge and their habits.

For advisors, this opportunity usually takes the form of internal training and frequent information sharing with peers and partners like Pershing. And investors are best served when their advisors share this information with them, as well.

The fraud landscape in 2020

An obvious place to start any security fraud training is with an updated list of current threats, their frequency, and their impacts. Today, that list is long and growing. It includes:

- Email compromise
- Malware
- Ransomware
- IRS impersonation scams
- Robocalls/unsolicited phone calls
- Sweepstake/lottery scams
- Elder financial abuse
- Text scams, targeting millennials on their smartphones



- Grandparent scams, where fraudsters pose as grandchildren
- Romance/companionship scams, where fraudsters act as romantic interests
- Identity theft
- CEO scams, where fraudsters pose as a CEO asking for high-value gift cards for employees
- Real estate scams

Real estate fraud is by far the fastest-growing threat today. Between 2016 and 2018, rates increased by 1,100%, says Hulstedt. And it's no wonder why. Fraudsters have learned they have more success when they time their transactions to coincide with real events happening in investors' lives – one typically surrounded by intense pressure and stress, like a real estate purchase.

Hulstedt says the exchange typically goes something like this: "Fraudsters pose as the investor and communicate with the advisor, either requesting a wire transfer directly or asking that it be sent to the title company. Then, 20 minutes before the house closing, they'll change the account number."

Nina Weiss, Chief Compliance Officer at Pershing, says ransomware cases, in which fraudsters hold an advisory firm's computing system hostage for money, are less prevalent today. But email hacking is on the rise, and investors are especially vulnerable when they reuse passwords.

With enough information, fraudsters may be able to copy signatures or intercept email threads. "Fraudsters will use bots to comb through literally every single document you have stored on your computer," says Hulstedt. "It's very, very easy." Hulstedt describes a case at Pershing he learned about recently: after three weeks of emails between investor and advisor, a fraudster took over the investor's email account and asked the advisor for a wire transfer of $400,000 (fortunately, the advisor called the investor to confirm before initiating the transaction).

Note that check fraud – a very slow process – is essentially off the radar. Most scams today are third-party requests for wire and electronic bank-to-bank (ACH) transfers, which are practically immediate.

Third-party fraud is also known as "true identity fraud," because it involves a fraudster impersonating an investor to open new accounts or take over existing ones without the investor's knowledge. The real end game for many fraudsters is to take those funds out of the United States, to countries that don't have extradition treaties, putting them out of reach from authorities, explains Hulstedt.

Remember what's at stake

Many advisors are busy and recognize their clients are busy too, which can lead some advisors to take shortcuts that they think will make the client happy. It's easy to argue, for example, that when a wire request appears to be consistent with what's happening in the investor's life, the risk of fraud is so small there's no need to follow up. Or that a client is very busy and doesn't like being interrupted, regardless of the reason.

The solution in both cases is to remember that fraudsters are smart and getting smarter. As an advisor, you can't afford to assume it can't or won't happen to you. And when it does, following up with a phone call is still the best safeguard available.

Yes, some clients might be irritated by this extra step, but setting the expectation – that there will always be a follow-up phone call, and it's for their protection – at the outset helps. "And in the end, it really comes down to which phone call you'd rather make," notes Weiss. "The one you're making to keep your clients' assets safe, or the one where you tell them they just lost $400,000."

Fraud training best practices

Even more important than the specific content of fraud training, whether targeted at advisors or investors, is the "tone from the top." That is, advisors who are true stewards of their clients' savings have leaders who do all they can to protect themselves from being victimized – because when fraud does occur, everyone is a victim.

With a culture built around proactive preparedness, firms are more likely to produce high-quality fraud training and information-sharing opportunities that do three things:

1. Give advisors and investors the information they need to avoid becoming victims of fraud
2. Emphasize the need and teach your advisors how to supplement this knowledge on their own on an ongoing basis
3. Coach your advisors on the specific mindset and habitual behaviors that will protect them from fraud

What's more, these learning opportunities will likely happen on an ongoing basis, with a cadence that matches the rapid pace of change in the fraud landscape.

What's in the box

As part of this package, Pershing includes timely data on fraud (e.g., number of successful attempts last year, dollar amounts, etc.) as well as specific guidance on cultivating good habits, both mental and behavioral. For example:

1. When fielding requests from elderly clients who might have diminished cognitive function, speak with a trusted contact person.
2. Elderly or not, always follow up on a client's emailed request for a transfer with a phone call to the client's number of record, regardless of the size of the transaction.
3. On the phone, ask for specifics: "Did you send me this request, for this amount, to this account?" Asking an additional authentication question is even better.
4. After you've called, sign an attestation to that effect.
5. If instructions change or there was a hand-off to a colleague somewhere in the process, document that the call was made.
6. Actively engage regulators and law enforcement in identifying and addressing fraud risks.

In addition, Pershing points our clients to valuable external resources like the OCIE's Cybersecurity and Resiliency Observations. This annual report offers additional suggestions on how advisors can stay informed between formal training – signing up for alerts from CISA, for example, checking the SEC's cybersecurity page, and participating in information sharing groups through industry organizations.

It's important to educate your clients as well. The goal is to develop an investment policy statement that identifies each client's short-, medium- and long-term goals, and sets the expectation that any request that deviates from the plan will trigger a follow-up phone call from the advisor.

Just like for advisors, frequent updates – via newsletter, blog post or both – are essential, as is a regular cadence of client meetings focused on best practices for detecting fraud. Advisors who take these steps help to preserve their reputations along with their clients' assets. And their businesses are positioned to grow as a result.

Choose the right course of action

When a fraudulent transaction does get through, the consequences can be severe. Hulstedt says the fraudster will immediately take the funds from the contra firm and move them to a different institution, and then it's up to the advisor to make the investor whole. "Error and omissions insurance doesn't always help," he cautions. "They won't cover you if you can't prove you took all the necessary precautions."

He's even heard of advisors having to write checks from their personal accounts. While an instance of fraud could be painful for a larger firm, depending on the dollar amount, it could force a smaller one to close its doors.

On top of the immediate financial risk, restoring an investor's assets after a fraud is a complex, lengthy process. Not only does the advisor have to replace all of the investor's trades from the transaction date, but money taken as taxes has to be recovered from the federal and state governments too. And when that process is complete, there's still the issue of reputational damage. Larger advisory firms will usually cut ties with an advisor implicated in fraud, not wanting to risk losing clients over a perceived lack of integrity. And solo advisors are particularly vulnerable. Once their names are sullied by an incident, keeping existing clients and acquiring new ones becomes a herculean feat.

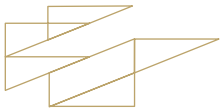
Learning how to protect your clients and your business from security fraud is much easier. But even more importantly, it will reinforce your role as a trusted advocate and enhance your relationships with clients.

As a custodian and a partner with stringent risk controls, Pershing is well positioned to keep you abreast of the latest fraud trends and help you share that information with your team. We hold regulatory and compliance webinars to share this information, and we're also able to keep you up to date on the latest news from regulators about the threats they see on the horizon.

At BNY Mellon's Pershing, we favor overcommunication, both internally and externally. There's a monthly compliance forum for every advisory firm we partner with – 503 in total – which is open to all their employees. We also send a weekly newsletter to all our clients, which includes the most current information we have on policy changes, recent developments in the industry as a whole and new scams on the horizon, as well as an annual presentation specifically around fraud.

We encourage each of our clients to call us on an ad-hoc basis with questions – we're always available to discuss best practices in this space. By working together, we can help you stay a few steps ahead of fraud, so you can focus on serving your clients.

[1] "Consumer Sentinel Network: Data Book 2018," Federal Trade Commission (February 2019) accessed on April 29, 2020.



Pershing

BNY Mellon's Pershing and its affiliates provide a comprehensive network of global financial business solutions to advisors, broker-dealers, family offices, hedge fund and '40 Act fund managers, registered investment advisor firms and wealth managers. Many of the world's most sophisticated and successful financial services firms rely on Pershing for clearing and custody; investment, wealth and retirement solutions; technology and enterprise data management; trading services; prime brokerage and business consulting. Pershing helps clients improve profitability and drive growth, create capacity and efficiency, attract and retain talent, and manage risk and regulation. With a network of offices worldwide, Pershing provides business-to-business solutions to clients representing approximately 7 million investor accounts globally. Pershing LLC (member FINRA, NYSE, SIPC) is a BNY Mellon company.

pershing.com

One Pershing Plaza, Jersey City, NJ 07399

WP-PER-WT-01-20