One Step Ahead: Help Protect Your Firm and Clients from Cyber Fraud

Actions for firms and investors to consider to help protect themselves against evolving cyber threats

INSIDE YOU’LL DISCOVER

• Growing threats to data security
• Common cyber fraud schemes
• Responsibilities of financial institutions
• Actions for firms to consider
• Supplemental resources

In Brief

**Cyber fraud is on the rise:** Massive data breaches and an increase in the use of online services and digital devices have made it easier for cybercriminals to execute successful attacks.

**Technical threats grow more sophisticated:** Cybercrime tools evolve with advances in technology. Today’s cybercriminals use an array of tools and techniques to breach victims’ security and monetize their access.

**Firms have responsibilities:** Federal regulation, and some state laws, require financial institutions—generally inclusive of firms registered as broker-dealers and/or investment advisors—to implement controls to prevent identity theft.

**Take action to protect your clients and firm.** While threats have intensified, fundamental cybersecurity practices still go a long way towards mitigating these risks.
Threats to data security intensify

As technology continues to evolve, cybercriminals are evolving just as fast, developing new ways to separate people from their assets. While the most common tactics used to compromise a victim’s security remain longtime nemeses such as malware and phishing, the latest variations of these tactics are more effective, complex, and difficult to spot. The consequences of failing to identify and mitigate these threats are significant.

Common cyber fraud schemes

Cybercriminals operating today apply a number of tactics to achieve their goals. Yet, most cyberattacks share commonalities in their objectives and execution. For example, attacks typically use one or more of the most common methods of circumventing your security—known as vectors of attack—in order to compromise financial accounts, email accounts, computer systems, or mobile devices. And then, once they have control, they will find ways to monetize that access.

The following sections offer an overview of the most common vectors of attack and asset loss scenarios that Fidelity’s security specialists continue to see.

The insights in this white paper are culled from in-depth conversations with the following Fidelity security specialists, each with more than 20 years of experience in fraud and information security:

- **Craig Devlin**
  Senior Vice President, Financial Intelligence Unit

- **Mark DiMarzio**
  Vice President, Financial Intelligence Unit, Fraud Surveillance

- **Michael Webber**
  Vice President, Financial Intelligence Unit, Cyber Investigations

Keep in mind that the following tips are intended to help you mitigate risk and are not intended as legal advice. There are many considerations to take into account when developing information security policies and procedures. It is advisable to consult legal counsel and/or other professional advisors with whom you work.
Vectors of Attack

Before they can gain control of your systems or accounts and ransack your assets, cybercriminals must subvert your defenses. In addition to simply exploiting vulnerabilities of unpatched systems, cybercriminals employ a variety of techniques to compromise the security of your financial accounts or computer systems.

- **Phishing:** Perhaps the most well-known vector of attack, phishing is essentially a fake electronic message designed to trick you into divulging information and/or granting access that you shouldn’t. Typically, it is a technique for attempting to acquire sensitive data such as financial account information or login credentials, through a fraudulent solicitation in electronic communication media such as email, websites, or social media. In these attacks, the perpetrator masquerades as a trusted, legitimate entity, often complete with a fake website that strongly resembles a real site. Solicitations may specifically prompt victims to provide this information—directly, or through the website—or they may direct victims to unknowingly install malicious software.

- **Vishing:** An abbreviation for voice phishing, vishing is another term for fraudulent phone calls designed to elicit the same sort of sensitive information that phishing does. While we’ve begun to cultivate a healthy societal skepticism around suspicious emails and other electronic communications, fraudulent phone calls remain a blind spot for many. This makes them an especially valuable technique for cybercriminals. Some use it to pose as tech support and request remote access to your computer, while others use it to compromise two-factor authentication protocols. To the extent that improving security against other schemes involves establishing and using two-factor authentication protocols, vigilance around fraudulent phone calls is critically important.

- **Credential Replay:** With the sheer volume of data breaches we’ve seen in recent years, and the subsequent billions of records exposed, a significant portion of the population may have compromised credentials. While some cybercriminals actively scan the web for unsecured databases, others will simply purchase stolen credentials from a third party. Once they acquire them, fraudsters may use those credentials to attempt to log in to other accounts. While it’s common practice for people to use a single password across many sites, doing so leaves them vulnerable to these kinds of attacks. The more a password is reused, the more chances there are for that password to be compromised or stolen.
• **Business Email Compromise**: While criminals may well seek to compromise business email accounts for other purposes, the intent of the fraud scheme known as Business Email Compromise is to take the deceit employed in phishing a step further. Rather than simply appearing to come from legitimate, known entities, these messages truly do! A typical example: cybercriminals will compromise a business email account and use that account to email money movement instructions to another employee of the company.

• **Malicious Software**: Like phishing, malware is a term that many are familiar with today. It’s used to advance a variety of goals, but at its essence, it is simply code inserted into a computer system to compromise that system’s security. The entry point to a system could be a click on a website, the opening of an email attachment, or even the installation of pirated or unknown software. Once installed, the software may capture and transmit your credentials the next time you enter them, or it may compromise system security protocols directly. The goal may be to gain access to sensitive information—such as Social Security numbers, financial account numbers, or passwords—as part of an identity theft-based scheme. Alternatively, the intent may be to steal or encrypt critical business data as part of a ransom scheme.

**Loss of Assets**

Once they have control of your accounts or systems, fraudsters can take advantage of that access. The losses incurred in such an attack can include those associated with the exposure of sensitive information, the potential loss of critical business data, and damage to systems. The detrimental effects of a data breach may be felt for years to come.

While there’s no shortage of ways in which cybercriminals can monetize stolen data, it’s the schemes involving theft of the victim’s assets that are often the most damaging. Here, we’ll explore three such schemes.

• **Fraudulent Money Movement**: The most common fraudulent money movement scenario involves transfers made by phone or electronically. Typically, in these situations, an individual’s email account has been compromised, giving the fraudster access to his or her personal information. Cybercriminals may also take additional steps to enhance the ruse, including establishing a fraudulent account in the victim’s name. In this approach, the fraudster transfers assets from the victim’s legitimate account to

---

**Did You Know?**
The 2019 annual report of the Federal Bureau of Investigation’s Internet Crime Complaint Center attributes $1.7 billion in reported US losses in 2019—and $26 billion, globally, since 2016—to Business Email Compromise schemes.

“In the case of financial services firms, fraudsters often assume the identity of their clients or their clients’ other advisors, such as attorneys or accountants. They inject themselves into authentic email threads at the last minute, to direct payments to accounts they control. Potential solutions include choosing unique passwords, requiring multi-factor authentication at login, limiting the amount of sensitive data stored in email accounts, and staying on alert for phishing activity,” says Mike Webber. He also points out that your employees can be victims of email compromise as well, and he asks that you notify Fidelity if that occurs. “Not only will we offer to lend technical expertise, if desired, we’ll also collaborate with you to develop a plan to protect any customers whose information might have been exposed to attackers.”
the fraudulent account, before quickly transferring the money out of that account too. Firm representatives are often concerned to learn that they may be held personally liable for a wire transfer that turns out to be fraudulent, if they failed to follow procedures (which typically include calling the client to verify transactions) before executing the transfer.

- **Fraudulent Trading:** Imagine having your assets traded on the stock exchange without your knowledge or permission, only to discover that those trades resulted in significant losses. This form of fraudulent trading typically occurs when an investor’s login credentials for his or her brokerage account are compromised. The cybercriminal then uses the compromised credentials to access the account and place trades in certain securities, to artificially inflate or deflate the price for a personal gain, which is then realized in a completely separate account.

- **Ransomware:** Ransomware is a type of malicious software (malware) that endeavors to gain leverage over the victim (rather than simply steal credentials) and use that leverage to extract a ransom payment. This may be accomplished by encrypting the data on the victim’s system and offering to decrypt the data for a fee. In these cases, the encrypted data is typically unrecoverable unless you pay the ransom or maintain reliable data back-ups. With the growing use of data back-up services, some cybercriminals have altered their approach to instead steal—and threaten to release—sensitive information. Of course, in either scenario, there’s no guarantee that payment will result in your data being accessible and safe again.

“Fraudulent trading continues to be an issue,” says Mark DiMarzio. “When financial services firms identify high levels of potentially fraudulent trading activity in a particular stock, we share that information with regulators. At Fidelity, we go a step further and share that information with a number of our competitors, so that everyone can be on alert.”

According to Mike Webber, preventing all ransomware attacks may be next to impossible. He recommends finding a trusted IT service provider who makes security a cornerstone of the relationship. “Working with a team that actively inventories your devices to ensure they are up to date will reduce the chances of the ransomware being able to spread. Having a team who can respond and of course, having a team who can quickly identify and mitigate problems will reduce the impact of those problems on your business operations.”

Webber also recommends that firms consider ransomware attacks to be potential privacy incidents. “Historically, ransomware blocked access to the victim’s data until a ransom was paid. Those with robust disaster recovery plans were able to recover fairly quickly and avoid paying the ransom. Recently, ransomware operators have reacted to this by stealing data (including credentials) before blocking access, and then threatening to publish the stolen data unless a ransom is paid.”
Responsibilities of financial institutions

In the context of these evolving and serious threats, it’s important to remember that financial institutions, as defined in the Fair Credit Reporting Act, have federally mandated responsibilities, as well as some applicable state laws, to protect clients.

The “Identity Theft Red Flags Rule,” known as Regulation S-ID, was issued jointly by the Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC) and became effective in 2013. It requires any SEC or CFTC-registered financial entity that directly or indirectly holds transaction accounts for its clients to develop and implement an identity theft protection program (ITPP).

What does it mean? Investment advisors, broker-dealers, and many other financial institutions are generally required to be in compliance by developing and implementing an identity theft protection program consisting of reasonable, board-approved compliance programs, with policies and supporting procedures to prevent, detect, and respond to any possible identity theft situations.

While Fidelity encourages all firms to remain vigilant in looking for signs of fraud, we suggest that you consult legal counsel to gain a full understanding of the rules and regulations that apply to your firm. This is especially important because current data protection and data breach notification laws vary from state to state.

Actions for firms to consider

In light of the significant and evolving cyber fraud and security risks that financial institutions face today, ask yourself: Are your security policies and procedures keeping up? Consider whether the following steps could help you to better protect your clients and your business.

1. Educate customers on proper third-party wire requests:
   Help clients understand the right practices involved in wire transactions—for their protection and yours. For example, faxes, voicemail messages, and emails should not be used to verify wire transactions. Customer education and awareness about your third-party wire requests may help make these types of money-movement controls more acceptable to your clients and actually encourage clients to play an active role in protecting their personal information and assets.
2. Establish, and regularly update, an employee education program on cybersecurity: Maintain a strong cybersecurity education program to keep all firm personnel abreast of the latest trends in cybersecurity and firm policies and procedures. You may also want to make cybersecurity a regular agenda topic for team meetings and have a plan in place to train new employees. Keep the threats associated with phishing top of mind, and ensure that employees have a mechanism to report suspicious emails, phone calls, and text messages.

3. Protect all user IDs and passwords: To protect against unauthorized access to your email, financial, or other important online accounts, avoid using one password on multiple sites. Add an additional layer of protection by using multi-factor authentication. Delete the login credentials of former employees, and periodically review the levels of access granted to current employees. As a further level of protection, consider establishing a policy to regularly reset employee passwords. Finally, don’t give broad-based entitlement to anyone who doesn’t need it.

4. Tighten controls around those places where two-factor challenges might be sent: Choose unique passwords and enable multi-factor authentication for your email account and your mobile carrier’s online portal. Create a passphrase or pin for your mobile account to prevent criminals from adding their phones to your account or changing contact information. Ensure that associates are aware that if cybercriminals can’t access their email or mobile account directly, they may call and attempt to convince them to read back the challenge codes.

5. Keep all of your devices up to date: Computer, tablet, and smartphone software should all be kept up to date. In most cases, financial malware and ransomware rely on vulnerabilities in systems that haven’t applied the latest security patches or antivirus definitions. Setup regular and automatic updates; intermittent updates leave your system vulnerable in between.

6. Limit employee access to sensitive client data to trusted networks and devices: Access sensitive data only through a trusted device and secure internet connection; avoid connecting to public or unsecured internet connections, unless you’re connecting through a Virtual Private Network (VPN).

7. Limit authorizations to move money: Exercise caution when authorizing individuals within your organization to execute money movements, and consider keeping the total number of authorized individuals small.

8. Align and configure resources to functions per security requirements: Restrict access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

9. Monitor and regularly review client account balances and transactions: If you see unusual transactions, immediately call the client to verify the transaction. Also, be sure to review any account profile changes. Again, if anything seems unusual, verify the changes directly with the client.

10. Consider your professional liability insurance: Professional liability insurance policies can help mitigate a range of risks. These include risks related to cybercrime, data breaches, errors and omissions made by employees, and alleged management malpractice related to an incident. Consider your coverage and how well it aligns with your firm’s risk profile.

To assist firms in applying the insights captured in this white paper to their practice, we’ve provided a number of supplemental resources over the following pages. For additional support, please contact your Fidelity relationship manager.
Make policies and procedures easy to understand and accessible to all staff

- Consider hiring a third-party facilitator or professional trainer to help initially present your policies and procedures.
- Ask associates to acknowledge that they have reviewed and understand the policies and procedures established by your organization. You may want to give them a test or have them sign a form to acknowledge that they fully understand the procedures.
- At a minimum, clearly document your organization’s policies and procedures. Have them accessible so that any member of your organization can refer to them at any time (e.g., on a shared drive with full staff access).

Conduct initial and ongoing staff training.

- If resources permit, you may want to create a short training video on various aspects of the policies.
- During regularly scheduled staff meetings, incorporate ongoing training and discussions about protection of client information. For example, add an agenda item to review one aspect of your organization’s policies or provide updates to any policies. Encourage attendees to share best practices regarding how they are implementing the policies.
- For particular topics, create checklists or hard cards that associates can easily reference. For example, create a hard card on policies and procedures for the disposal of information.

Train all new associates.

- Offer training as part of the onboarding process for new associates.
- Have your organization’s International Organization for Standardization (ISO) check in with new associates after a short onboarding period (e.g., 30 days) to be sure they understand how to implement policies and are able to ask questions.
While you may be taking all the necessary steps to protect your firm from cyber fraud, we encourage you to consider developing an ongoing communications program to help your clients better understand the ways they can protect themselves from cyber threats. The sample resources that follow are intended to help you deliver your message effectively. On this and the following pages, you’ll find:

- A sample cyber fraud client communications plan
- A sample client letter you can consider and customize to your unique needs
- A sample investor protection checklist to aid client awareness of action items across six important areas

### SAMPLE CYBER FRAUD CLIENT COMMUNICATION PLAN

<table>
<thead>
<tr>
<th>TIMING</th>
<th>AUDIENCE</th>
<th>SUGGESTED STEPS TO CONSIDER</th>
</tr>
</thead>
</table>
| Immediately  | All clients  | • Send customized copies of the client letter and investor protection checklist, found at the back of this guide, to all clients.  
• Consider a proactive phone call to clients you feel could benefit from a conversation about the checklist items. |
| Ongoing      | All clients  | • During your annual review meetings, remind all clients of the importance of protecting their personal information. Allow time in your discussion to answer any questions they may have, and give them another copy of the checklist as a reminder.  
• Communicate new developments or best practices to your clients when you learn of them. |
| Onboarding   | New clients  | • When onboarding new clients, provide them with a copy of the investor protection checklist and client letter. |
Dear [Insert Client Name]:

Keeping your information secure from criminals is a top priority for our firm. To better protect you and your accounts from cybersecurity threats, we continuously review security procedures to ensure that we are following best practices recommended by the custodians, financial institutions, and industry experts with whom we work.

While we feel we are taking clear and actionable steps in our own firm's security measures, cyber fraud continues to escalate, is becoming more sophisticated, and is ever changing. These threats take various forms, including email scams (e.g., phishing), where criminals obtain investors’ identity and use that information to commit various forms of wire fraud. The attachment to this letter describes these phishing scams and other tactics we believe investors should be aware of.

We are encouraging our clients to embrace a series of measures to help protect their identity and mitigate potential security risks. The attached investor protection checklist outlines some best practices for investors across six key areas to help you:

- Protect all passwords.
- Manage your devices.
- Surf the web safely.
- Protect information on social media.
- Protect your email accounts.
- Safeguard your financial accounts.

Please carefully review this checklist with all members of your household. We also ask that you do the following:

- If you change a current address, notify us so that we can update our records.
- If you suspect that your email or Fidelity account has been compromised, please call us immediately.

Do not hesitate to contact us with questions or concerns about how we protect your accounts or the steps you and your family can take to better protect yourselves and mitigate risk. As always, we appreciate the opportunity to help you achieve your financial goals.

Sincerely,

[Insert Representative Name]
Common tactics used to steal login credentials

Some of the most common tactics criminals use to compromise a victim’s identity or login credentials are described below. After gaining access to an investor’s personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the investor protection checklist are intended to help you and your family better protect yourselves against such activity.

**Malware**
Using malicious software (hence, the prefix “mal” in malware), criminals gain access to corporate and private computer systems and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.

*How it works:* While malware can be inserted into a victim’s computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email attachment.

**Phishing**
Phishing is a popular tactic used by cyber criminals to steal account information or login credentials. It is essentially a fake electronic message designed to trick you into divulging information and/or granting access that you shouldn’t. This is often accomplished with the help of a fake website that strongly resembles a real site.

*How it works:* Masquerading as a known entity, or one with which the victim may have a financial relationship (e.g., a bank, credit card company, brokerage company), the criminals lure victims into opening email links or attachments. Doing so may direct victims to provide sensitive information on a fake website, or it may install malware to capture login and account information.

**Credential Replay**
It’s common practice for people to use one password on many sites. However, doing so leaves people vulnerable to credential replay attacks.

*How it works:* Attacks occur when a criminal obtains the password for one compromised account and then tries to use it to log in to other accounts. The more a password is reused, the more chances there are for that password to be compromised or stolen.
**SAMPLE CYBER FRAUD RESOURCES**

**Investor protection checklist**

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

<table>
<thead>
<tr>
<th>TOPICAL AREA</th>
<th>ACTIONS TO CONSIDER</th>
<th>CHECK WHEN COMPLETED</th>
</tr>
</thead>
</table>
| **Manage your devices.** | • Install the most up-to-date antivirus and antisyppware programs on all devices and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scans, which may not provide maximum protection to your device.  
• Access sensitive data only through a trusted device and secure Internet connection; avoid use of public Internet connections other than through a Virtual Private Network (VPN).  
• If you have children, set up a separate computer they can use for games and other online activities.  
• Keep operating systems and software up to date (PCs, laptops, tablets, smartphones). Many updates are made to resolve recently identified security risks.  
• Do not install pirated software. It often contains security exploits.  
• Frequently back up your data in case of ransomware attacks. | □ I've reviewed and understand all the items in this topical area.  
□ I've taken action for those that apply to my situation. |
| **Protect all passwords.** | • Avoid storing passwords in email folders or un-encrypted files on your computer. Consider using a password manager program instead. These programs help generate and manage complicated passwords.  
• Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity.  
• Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships, and avoid using a single password across multiple sites.  
• Utilize multi-factor authentication, especially for financial and email accounts. | □ I've reviewed and understand all the items in this topical area.  
□ I've taken action for those that apply to my situation. |
| **Surf the web safely.** | Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels or coffee shops. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data directly, without the proper protection of a secure VPN connection. | □ I've reviewed and understand all the items in this topical area.  
□ I've taken action for those that apply to my situation. |
| **Protect information on social media.** | Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays, or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that criminals will use to learn critical facts about people. | □ I've reviewed and understand all the items in this topical area.  
□ I've taken action for those that apply to my situation. |
<table>
<thead>
<tr>
<th>TOPICAL AREA</th>
<th>ACTIONS TO CONSIDER</th>
<th>CHECK WHEN COMPLETED</th>
</tr>
</thead>
</table>
| Protect your email accounts. | • Delete any emails that include detailed financial information beyond the time it’s needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account.  
• Use secure data storage programs to archive critical data and documents.  
• Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action.  
• Establish separate email accounts for personal correspondence and financial transactions.  
• Choose a unique password and utilize multi-factor authentication.  
• Review all emails carefully before clicking on links or attachments. | ☐ I’ve reviewed and understand all the items in this topical area.  
☐ I’ve taken action for those that apply to my situation. |
| Safeguard your financial accounts. | • Consider contacting the three major credit bureaus to add a "security freeze" and prevent new accounts being opened in your name:  
  – **Equifax**: 800-685-1111  
  – **Experian**: 888-397-3742  
  – **Transunion**: 888-909-8872  
• Lock down personal credit reports with Experian®, TransUnion®, and Equifax®. Proactively enroll in an identity theft protection service to protect personal data.  
• Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.  
• Never send account information or personally identifiable information over email, chat, or any other unsecured channel.  
• Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website’s URL into the browser yourself.  
• Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate. | ☐ I’ve reviewed and understand all the items in this topical area.  
☐ I’ve taken action for those that apply to my situation. |
For additional information and resources, please visit our website or contact your Fidelity representative.