NORTHERN TRUST

FRAUD SCAMS AND ACTION STEPS SUMMARY

A significant increase in fraud makes it more important than ever to recognize the signs of suspicious activity and to take precautions to protect yourself.

LOOK FOR COMMON SCAMS

1. **Impersonation** – Fraudster poses as a representative from a company you trust (via phone, text or email) and creates urgency to gain access to your personal information.
2. **Business Email Compromise** – Criminal sends an email message that appears to come from a known email address and to be a legitimate request for you to send money.
3. **Account Takeover** – Scammer insists that you download software or allow them to remotely log in to your devices to assist with an urgent issue.

TAKE STEPS TO PROTECT YOURSELF

PERSONAL INFORMATION	TRANSACTIONS	YOUR COMPUTER AND DEVICES
• Frequently update your password (every 60-90 days) and user ID (annually). • Use strong passwords and do not share them. • Never give out your credentials. Northern Trust will never contact you and ask for your User ID, PIN, Password or authorization codes. • Never provide information to an unsolicited contact via email or telephone. • Use care when engaging with social media and avoid revealing sensitive personal information. • Protect physical checks by keeping them secure and locked. Avoid using a public mailbox for mailing.	• Always verbally verify payment via a trusted or known phone number as emails are an unsecure method of communication. • Use caution and make sure that you know the recipient when sending money via wire or Zelle®. • Be wary of urgent requests or being rushed to make a decision to send money. • Be suspicious when fear is being used to convince you to move money (relative has been arrested, computer has been hacked or accounts have been frozen).	• Never allow anyone you don't know to access your computer remotely. • For your security, always log out when you have completed your online financial activities. • Learn to avoid Phishing (legitimate-looking email messages that attempt to gather personal and financial information, spread viruses or install malicious code). • Go directly to the website you are attempting to reach rather than clicking on embedded links in emails. • Install up-to-date anti-virus and anti-spyware programs on your home computers. • Download security patches and software/operating system updates in a timely fashion. • Use caution when using unsecure wireless hotspots in public spaces.

OTHER ACTION STEPS TO CONSIDER

- Enroll in Private Passport.
  - Ability to actively monitor your accounts.
  - Access your most recent statements through a central, secure online location so you never worry about missing or losing a statement.
  - Receive paperless statements to increase security and protect your identity by decreasing hard copy documents with personal information.
  - Eliminate need for physical check stock by using secured electronic money movement features such as Bill Pay, Zelle® and transfers across Northern trust and external accounts.
  - Regularly reconcile your bank statements and set up alerts to monitor your accounts for unexpected activity.
- Talk with your relationship manager about setting up letters of direction for routine or recurring transactions.
- Visit NorthernTrust.com/security to learn more.

Immediately contact your Northern Trust team if you become aware of fraudulent activity or see something suspicious.