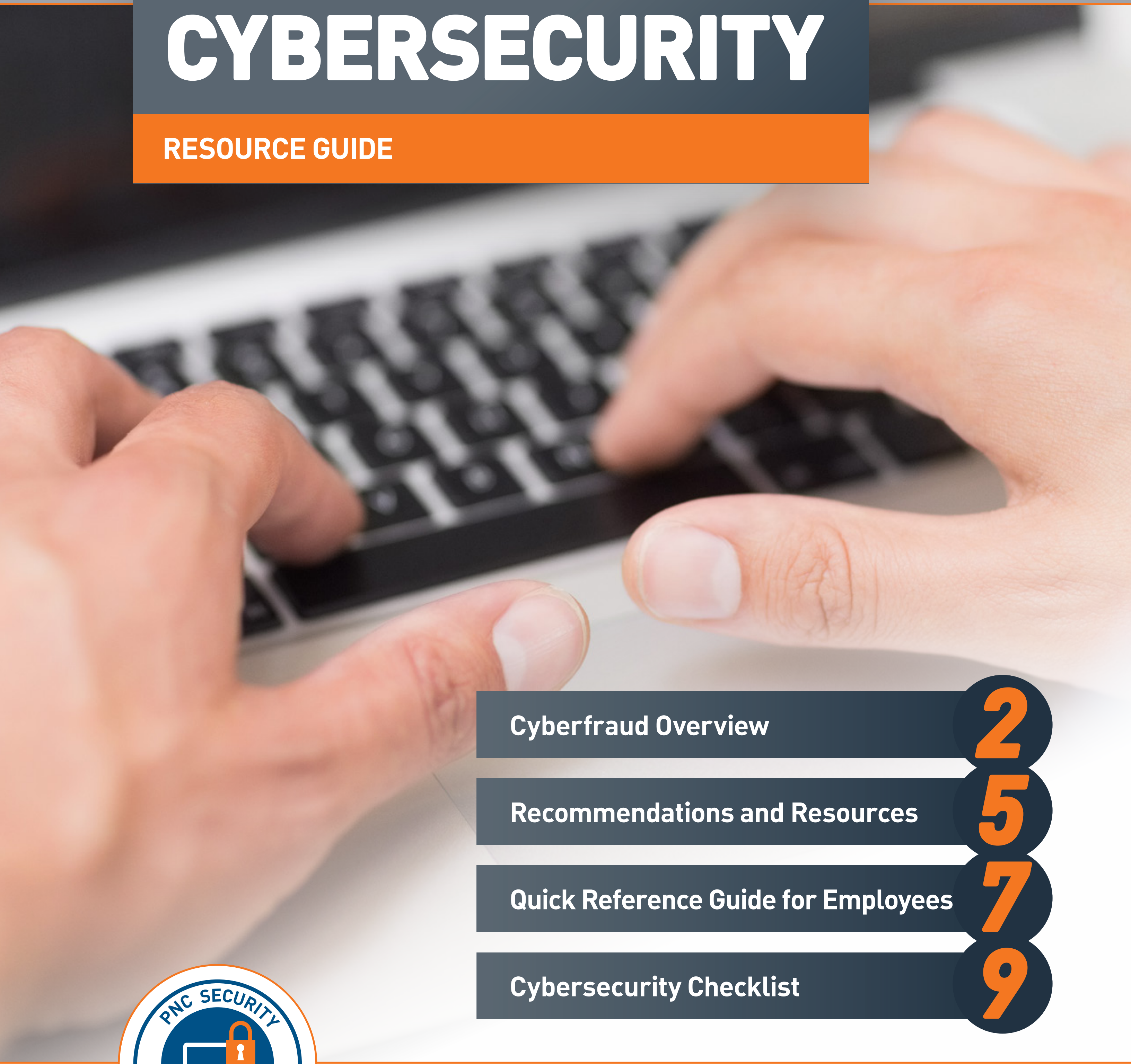
INSTITUTIONAL ASSET MANAGEMENT

CYBERSECURITY

RESOURCE GUIDE



PNC SECURITY AWARENESS

PNC INSTITUTIONAL ASSET MANAGEMENT

AWARENESS OF CYBER THREATS FOR FRAUD

Payments, distributions and transfer fraud attempts are widespread across all industry types as a result of email compromises and financial malware infections. Understanding how these fraud schemes are designed to infiltrate/compromise your business and taking action to prevent them are critical to your defensive strategy.

It is imperative that employees and third parties with access to funds movement services are aware of these fraud schemes and can recognize potentially fraudulent or malicious activity against their email or I-Hub login credentials. These are very real threats, and we encourage you to educate staff throughout your organization along with any third-party I-Hub users.

ATTEMPTED FRAUD VIA EMAIL COMPROMISE

Cybercriminals initiate fraudulent payment or transfer requests, or requests to change payment instructions, from email accounts that appear to be from an organization executive (such as the CEO or CFO) or from a known external partner, such as an investment consultant. The fraudulent "From" email address may be a fictitious account in the executive's name, or it may be a slight variation of a legitimate consultant's email address, both of which can trick the recipient into believing that the communication is valid. It is also possible that the sender's legitimate email account has been compromised, making it essential that all I-Hub users are able to recognize the characteristics of a fraudulent request.

Also be mindful that even when an email account is not compromised, there is quite a lot of information available in open source records (e.g., social media, public records) that cybercriminals can obtain easily in developing such schemes. For example, large endowments and foundations, such as for universities or hospitals, are disclosed in public filings. Cybercriminals can access these records, register a website impersonating the legitimate investment consultant, and initiate communication with the university/hospital requesting investment funds to be transferred out via wire. Oftentimes, the cybercriminals will wait several months before initiating contact and use open source records to identify internal investment managers or any third parties working with the organization to manage their assets.

Another email impersonation fraud scam targets retirement plan participant direct deposits. Hacked or spoofed email accounts are used to request changes to the plan participant's direct deposit information. As with all email requests relative to distributions, you should confirm them with the requestor at a known telephone number.

RECOGNIZE THE TYPICAL EMAIL FRAUD REQUEST SCENARIOS

- A plan participant requests changes to payment instructions for an upcoming payment.
- An email appears to be from an organization executive to initiate an urgent transfer — typically for an acquisition, investment, payment or some other confidential reason.
- An email appears to be from an organization executive delegating authority to an attorney or other external party for the purpose of providing payment instructions.

RECOGNIZE THE WARNING SIGNS OF AN EMAIL COMPROMISE

- Fraudulent emails will typically request that the recipient take one or more of the following actions:
  - Bypass established initiation and approval procedures.
  - Keep the payment, distribution or transfer confidential.
  - Provide immediate confirmation (to requestor) when the payment is executed.
  - Communicate with the requestor only via email.
- The requests will often warn of serious repercussions for failure to comply.
- Many times the executive appearing to be requesting the payment is out of the office or unavailable (which the fraudsters have previously determined).
- The request varies from the typical payment or distribution pattern for the organization or the sender.
- The recipient should ask:
  - Does the organization executive routinely communicate these requests via email?
  - Is the request consistent with other emails from the sender?
  - Are the email signature and tone consistent with other emails from the sender?

TAKE ACTION TO HELP PROTECT AGAINST THIS THREAT

- Train your I-Hub users to be vigilant when reviewing and confirming these requests, especially those conveying a sense of urgency and/or insisting on secrecy.
- Establish formal policies, procedures and controls for all payment, distribution and transfer initiation requests.
  - Executive management should communicate and follow the policies and procedures.
  - Employees should be trained and empowered to recognize requests that deviate from the established procedures and obtain confirmation of such requests from the requestor in person or via a known telephone number.

DANGEROUS FINANCIAL MALWARE INFECTIONS

Phishing emails, often with generic subject lines such as “Invoice” or “Resume,” can contain dangerous financial malware variants in attachments or links.

Once the malware has been installed on a computer, it redirects a user’s online banking sessions to a malicious site that harvests access credentials, such as User ID, Operator ID, Password and Security Codes.

It is important to know that **financial malware is often not detected by antivirus software**.

RECOGNIZE THE WARNING SIGNS OF A MALWARE INFECTION WHEN USING I-HUB

- A user may experience one or more of the following from a malware infection:
  - Inability to log in due to screens that delay or redirect the typical login experience.
  - Being prompted to provide their security codes repeatedly or presented with a “System Unavailable” message during the login process.

    I-Hub will never prompt an operator to enter login credentials (including security codes) multiple times during the login process.
  - Receiving instructions to have another operator log in from the same computer as part of a security process or to reactivate/unlock another ID.

    PNC will never request that an I-Hub operator have another I-Hub operator log in from the same computer during an online banking session or require another operator to log in from the same computer to reactivate/unlock an ID.
  - Experiencing problems logging in to I-Hub. Subsequently, the operator may receive a call from someone purporting to be from PNC asking for login credentials (such as a password) or asking to have another operator log in from the same computer in order to resolve the problem.

PNC will never:

- Call you or send you an email or text message asking for your I-Hub credentials or your contact information.
- Call you to advise you of new security procedures for your I-Hub login; we will always place this information, in advance, on the I-Hub homepage (and you may receive a corresponding email if you subscribe to receive email alert messages).

You should not respond to any communication requesting your sensitive information and should report any occurrences to the I-Hub Support Team immediately at 877-636-9703 (Hours: 8 a.m. – 5 p.m. ET, Monday–Friday).

TAKE ACTION TO HELP PROTECT AGAINST THIS THREAT

- Verify the authenticity of the communication before opening attachments or clicking on links in any emails that are unexpected or from an unknown sender. Contact the sender at a known telephone number to confirm that the suspicious content was indeed sent to your attention.
- Installing anti-malware software is highly recommended.
  - **PNC offers IBM® Security Trusteer Rapport® as a no-cost, optional security tool** that can help safeguard your I-Hub login credentials from phishing attempts and to remove certain malware from your computer. Download and install Trusteer Rapport by visiting the link below.

LINK: pnc.com/en/security-privacy.html

If you experience any of these scenarios or if any similarly suspicious behaviors occur during an I-Hub session, your computer may be infected with malware. Please contact the I-Hub Support Team immediately at 877-636-9703 (Hours: 8 a.m. – 5 p.m. ET, Monday–Friday) or PNC.I-HUB.support@pnc.com.

AVOID BEING A STATISTIC

INCREASE THE SECURITY OF COMPUTERS AND PASSWORDS

- Use strong passwords.
- Don’t recycle passwords.
- Recommend password changes every 30–90 days.
- Verify that antivirus software is current and is set to update automatically.
- Install Trusteer Rapport Malware Detection Software.

EDUCATE ALL I-HUB USERS

- Institute cybersecurity and awareness training for all employees, consultants and other third-party administrators.
- Communicate new cyber trends and alerts.
- Conduct fake email campaigns to test users’ ability to recognize phishing emails.

THE STATISTICS

74% of organizations were targets of payments fraud in 2020.

66% of organizations experienced check fraud in 2020.

76% of organizations were exposed to business email compromise (BEC) in 2020.

34% of organizations were subject to ACH debit fraud in 2020.

70% of organizations implemented controls to protect against BEC scams in 2020.

Source: 2021 AFP Payments Fraud and Control Survey — Report of Survey Results

IMPLEMENT FRAUD SOLUTIONS

Our professionals can work with you to understand your organization's needs and recommend specific services to help your organization enhance its fraud prevention posture. Below are just some of the services that I-Hub offers:

- **Self-Directed Asset Trading**
  For clients who direct trades, they can process mutual funds, equities and fixed income asset trades.
- **Benefit Payments for Retirement Plans**
  Users can initiate and manage benefit payments for retirement plans. Plan sponsors can also get inquiry access and reporting through our PayWeb application.
- **Cash Management**
  Users can initiate and directly manage cash processing transactions such as withdrawals, deposits and transfers.
- **Reporting Capabilities**
  Customizable reporting of key information, including account holdings, transactions and tax lots, through our I-Link application to stay on top of account management.
- **Approval Tailored to Your Organization's Needs**
  Customizable approval flows for transaction requests allow your organization to tailor the authorization process based on user entitlements.
- **IBM® Security Trusteer Rapport®**
  A software application that provides an additional layer of security designed to help protect your login credentials, including your I-Hub password.

ENHANCE INTERNAL POLICIES & PROCEDURES

- Establish formal policies and procedures for payment processing and investment changes. For example:
  - Require I-Hub usage or have a verbal callout verification process for any payment or distribution instruction change request.
  - Require secondary approval (internally) for all withdrawals, transfers and other significant changes.
  - Use a third layer (e.g., executive approval) for high-dollar transactions.
- Review I-Hub security features, controls and operator entitlements:
  - Confirm that funds movement entitlements are appropriate for each employee's job function.
  - Review notification settings to ensure that withdrawals exceeding certain thresholds generate emails to all authorized users.
  - Segregate payment initiation and payment approval functions.

ADDITIONAL RESOURCES

PNC Security & Privacy

Information and videos about current fraud trends and protocols

LINK: pnc.com/en/security-privacy.html

PNC Ideas, Insight & Solutions

Articles, white papers and insights

LINK: pnc.com/ideas

FBI Internet Crime Complaint Center

Business and consumer fraud alerts, tools to report fraud to the FBI, frequently asked questions, tips and considerations

LINK: www.ic3.gov
www.ftc.gov
www.staysafeonline.org

FDIC's "A Bank Customer's Guide to Cybersecurity"

What consumers can do to help protect themselves from cyberfraud

LINK: https://www.fdic.gov/consumers/consumer/news/cnsum18/cybersecurity.html

PNC INSTITUTIONAL ASSET MANAGEMENT

CYBERSECURITY & AWARENESS

QUICK REFERENCE GUIDE

PRINT THIS PAGE FOR EASY REFERENCE.

VERIFY AND VALIDATE

- Verify email payment/distribution or payment/distribution change requests in person or via a known phone number.
- Do not reply to an email to validate a request.
- Do not use contact information provided in an email to validate a request.
- Verify authenticity of an email before opening attachments or clicking on links.

PROTECT INFORMATION

- Be cautious about sharing information via social networking sites.
- Limit executive contact information on your organization's website.
- Do not confirm or provide personal information in response to an email or a text message.
- Do not give out personal information over the phone to unknown sources.
- Do not share executive travel/vacation schedules with unknown sources.

DETECT BUSINESS EMAIL COMPROMISE (BEC)

- Be suspicious of any vendor change in payment instructions.
- Inspect email header and look for alterations (e.g., the use of two "V's" to look like a "W").
- Be mindful that the "From" name in your inbox can mask a fraudulent email account.
- Be suspicious of messaging that is urgent and/or that requests secrecy.
- Be suspicious when the sender advises that they can be reached only via email.
- Be suspicious of emails requesting that payments or transfers be sent to new accounts or mailing addresses.
- Be sensitive to emotionally charged communications.
- Be suspicious of emails with generic subject lines (e.g., "Your Documents" or "Invoice").

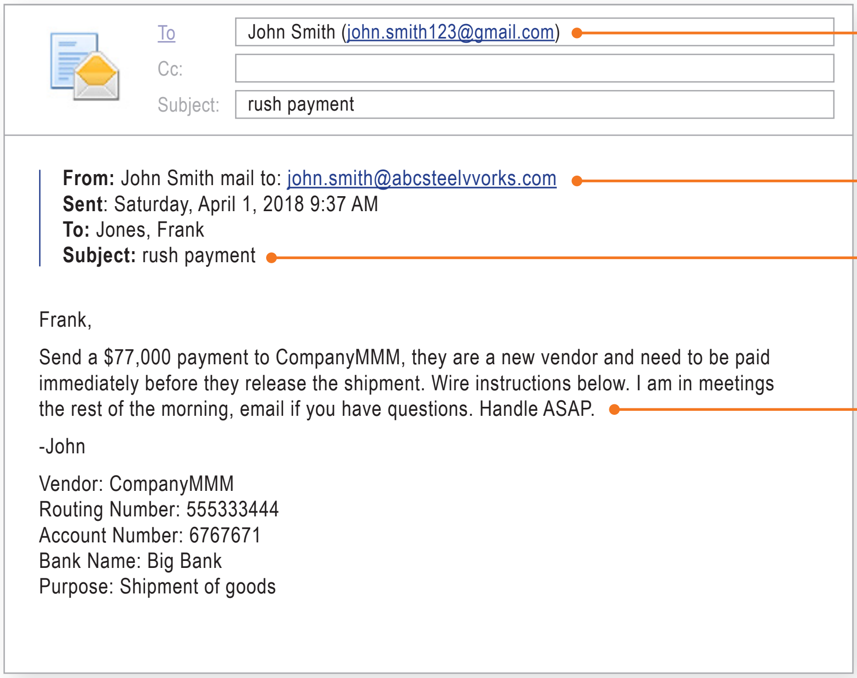
COMMON BUSINESS EMAIL COMPROMISE RED FLAGS

⚠	**COMPROMISED INTERNAL EMAIL**	**COMPROMISED VENDOR EMAIL**	**FINANCIAL MALWARE**
Appears to Come From	Organization Executive	Existing Vendor	External Business Partner or Vendor
Red Flags	• Urgent, confidential request • Requestor can be reached only via email	• Requests payment using new account or payment instructions	• Email request to log in to online banking using link provided in the email • Online banking login: - Multiple prompts for password/token - Requires second user to log in on same computer
Result	• Payment sent to fraudster	• Payment sent to fraudster • Vendor relationship disrupted	• Fraudster obtains login credentials and initiates payment on real bank site

EXAMPLE

PRINT THIS PAGE FOR EASY REFERENCE.

FRAUDULENT “SPOOFED” EMAIL



To: John Smith (john.smith123@gmail.com)

Cc:

Subject: rush payment

From: John Smith mail to: john.smith@abcsteelvvorks.com
Sent: Saturday, April 1, 2018 9:37 AM
To: Jones, Frank
Subject: rush payment

Frank,

Send a $77,000 payment to CompanyMMM, they are a new vendor and need to be paid immediately before they release the shipment. Wire instructions below. I am in meetings the rest of the morning, email if you have questions. Handle ASAP.

-John

Vendor: CompanyMMM
Routing Number: 555333444
Account Number: 6767671
Bank Name: Big Bank
Purpose: Shipment of goods

When you “Reply All,” the email address appears differently

The “w” in the company name is spelled with two v’s

It’s an urgent request

New wire instructions not currently on file

YOUR CYBERSECURITY CONSIDERATIONS

COMPUTER AND PASSWORDS	✓
⚠ Has your organization downloaded Trusteer Rapport malware detection software?	
Does your organization require regular password changes every 30 to 90 days?	
Is your organization's antivirus software up to date, enabled and set to auto-update?	
Does your organization use any other fraud surveillance tools or services?	
ENHANCED INTERNAL POLICIES AND PROCEDURES	
⚠ Has your executive team reinforced with your asset management team in writing that all employees and third-party consultants must strictly follow the transfer and distribution processing requirements, policy and procedures?	
Does your organization have formal policies and procedures in place for requesting transfers, distributions or payments from your investment account?	
Does your organization require secondary approval for all payment or transfer requests?	
Does your company require secondary approval for changes to payment or transfer instructions in bank and third-party systems?	
Does your company require third-layer, executive approval for high-dollar transactions?	
VERIFY AND VALIDATE	
⚠ Are email payment or transfer change requests confirmed by phone using contact information on file (vs. contact information provided in the email request)?	
⚠ Are distribution or wire transfer requests sent via email from internal executives/managers confirmed verbally using contact information on file (vs. contact information provided in the email request)?	
INFORMATION PROTECTION	
Does your organization have a social media policy that employees must read and sign?	
Does your organization limit executive contact information on the company website?	
Does your organization prohibit giving out personal information, including executive travel schedules, over the phone to unknown sources?	
BUSINESS EMAIL COMPROMISE (BEC) DETECTION	
Do your employees review emails for possible fraudulent payment/transfer requests, verifying headers, addresses and generic subject lines?	
Are your employees cautious about email requests that are urgent and emotionally charged and when the recipient is available only via email?	
EMPLOYEE/THIRD PARTY EDUCATION AND AWARENESS	
Do all I-Hub users with authorization to initiate and approve payment requests receive cybersecurity training?	
Do you provide regular alerts and updated training for employees and third-party consultants regarding cyber trends?	

READY TO HELP

If you suspect or experience fraudulent activity, please contact the I-Hub Support Team immediately at **877-636-9703** (Hours: 8 a.m. – 5 p.m. ET, Monday–Friday) or **PNC.I-HUB.support@pnc.com**.

Or, if you would like to learn more about protecting your organization from fraud, contact your PNC Relationship Manager.

The information and materials were prepared for general information purposes only and are not intended as legal, tax or accounting advice or as recommendations to engage in any specific transaction, including with respect to any securities of PNC, and do not purport to be comprehensive. Under no circumstances should any information contained in these materials be used or considered as an offer or commitment, or a solicitation of an offer or commitment to participate in any particular transaction or strategy. Any reliance upon any such information is solely and exclusively at your own risk. Please consult your own counsel, accountant or other advisor regarding your specific situation. Any opinions expressed in these materials are subject to change without notice.

By clicking "Download," you will be directed to a third-party website hosted by Trusteer, a third party that is not affiliated with PNC Bank. While this software is a valuable addition to your fraud prevention strategy, PNC Bank will not be responsible for the content or effectiveness of the services associated with Trusteer's software.

IBM and IBM Security Trusteer Rapport are registered trademarks of IBM in the United States.

The PNC Financial Services Group, Inc. ("PNC") uses the marketing name PNC Institutional Asset Management® for the various discretionary and non-discretionary institutional investment, trustee, custody, consulting, and related services provided by PNC Bank, National Association ("PNC Bank"), which is a **Member FDIC**, and investment management activities conducted by PNC Capital Advisors, LLC, an SEC-registered investment adviser and wholly-owned subsidiary of PNC Bank. PNC uses the marketing names Retirement 1-on-1® and PNC Financial Wellness Achievement Center℠ for employee education services provided by PNC Bank. PNC does not provide legal, tax, or accounting advice unless, with respect to tax advice, PNC Bank has entered into a written tax services agreement. PNC Bank is not registered as a municipal advisor under the Dodd-Frank Wall Street Reform and Consumer Protection Act.

"PNC Institutional Asset Management" and "Retirement 1-on-1" are registered marks, and "PNC Financial Wellness Achievement Center" is a service mark, of The PNC Financial Services Group, Inc.

Investments: Not FDIC Insured. No Bank Guarantee. May Lose Value.

PNC
INSTITUTIONAL
ASSET MANAGEMENT