

CORPORATE & INSTITUTIONAL BANKING

CYBERSECURITY

RESOURCE GUIDE

Cyberfraud Overview

2

Recommendations and Resources

5

Quick Reference Guide for Employees

7

Cybersecurity Checklist

10



AWARENESS OF CYBER THREATS FOR PAYMENTS FRAUD

Payments 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 with access to funds movement services are aware of these fraud schemes and can recognize potentially fraudulent or malicious activity against their email or PINACLE® login credentials. These are very real threats, and we encourage you to educate staff throughout your organization.

ATTEMPTED PAYMENTS FRAUD VIA EMAIL COMPROMISE

Cybercriminals initiate fraudulent payment requests, or requests to change payment instructions, from email accounts that appear to be from a company executive (such as the CEO or CFO) or from a known external partner, such as a supplier. 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 supplier 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 employees are able to recognize the characteristics of a fraudulent payment 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 (social media, public records) that cybercriminals can obtain easily in developing such schemes. For example, large construction contracts, such as for universities or hospitals, are disclosed in public filings. Cybercriminals can access these records, register a website impersonating the legitimate contractor, and initiate communication with the university/hospital introducing a “new” accounts receivable contact and account number set up specifically for this contract. Oftentimes, the cybercriminals will wait several months before initiating contact and use open-source records to identify accounts payable personnel.

In such schemes, the cybercriminals don’t need to know the amount of the upcoming payment or even the projected date for the payment. Instructions sent typically state that “All payments going forward should be made to the new account number and to the attention of the new accounts receivable contact.” As construction contracts are typically paid in net 30-, 60- or 90-day increments, often the victims are unaware of the fraud until weeks or months have passed, making recovery of funds extremely difficult. These types of schemes often involve losses in excess of \$1 million.

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





RECOGNIZE THE TYPICAL EMAIL FRAUD REQUEST SCENARIOS

- A supplier requests changes to payment instructions for an upcoming payment.
- An email appears to be from a company executive to initiate an urgent payment — typically for an acquisition, investment, payment or other confidential reason.
- An email appears to be from a company 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 payment initiation and approval procedures.
 - ▶ Keep the payment 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 pattern for the company or the sender.
- The recipient should ask:
 - ▶ Does the CEO (or other executive) routinely communicate payment 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 employees to be vigilant when reviewing and confirming payment requests, especially those conveying a sense of urgency and/or insisting on secrecy.
- Establish formal policies, procedures and controls for all payment initiation requests and additions/changes to your accounts payable system.
 - ▶ 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, Security Codes and Token.

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 PINACLE®

• 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 token passcode or security codes repeatedly or presented with a “System Unavailable” message during the login process.

PINACLE will never prompt an operator to enter login credentials (including a token passcode or 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 a PINACLE operator have another PINACLE 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 PINACLE. Subsequently, the operator may receive a call from someone purporting to be from PNC asking for login credentials (such as a password or token passcode) 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 PINACLE credentials or your contact information.

- Call you to advise you of new security procedures for your PINACLE login; we will always place this information, in advance, in the PINACLE Message Center (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 TM Client Care immediately at 800-669-1518.

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.
- Use a dedicated computer with no email access and limited internet access for payment initiation or online banking access.
- 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 PINACLE login credentials from phishing attempts and to remove certain malware from your computer. Download and install Trusteer Rapport by visiting the link below. To learn more, please visit the PINACLE Security Center by clicking on the blue shield icon located at the upper-right corner of any PINACLE page.

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

- ▶ **If you experience any of these scenarios or if any similarly suspicious behaviors occur during a PINACLE session, your computer may be infected with malware. Please contact Treasury Management Client Care immediately at 1-800-669-1518, Option 1.**

AVOID BEING A STATISTIC

INCREASE THE SECURITY OF COMPUTERS AND PASSWORDS

- Use strong passwords.
- Don't recycle user IDs or passwords.
- Require password changes every 30 to 90 days.
- Verify that antivirus software is current and is set to update automatically.
- Install Trusteer Rapport Malware Detection Software (additional information is available in the PINACLE Security Center).
- Use dedicated computers for PINACLE access (no email and restricted website access).

EDUCATE EMPLOYEES

- Institute cybersecurity and awareness training for all employees.
- Communicate new cyber trends and alerts.
- Conduct fake email campaigns to test employees' ability to recognize phishing emails.



THE STATISTICS

The Top 5 types of cyber-related crimes in 2022 were phishing, personal data breach, nonpayment/nondelivery scams, extortion and tech support scams.

\$2.7 billion in losses related to business email compromise (BEC) attacks were reported to the FBI's Internet Crime Complaint Center (IC3).

The **second largest** loss type in the United States is attributed to BEC attacks.

BEC attacks have **increased** consistently over the past three years.

Source: FBI Internet Crime Report 2022

IMPLEMENT PAYMENTS FRAUD SOLUTIONS

Our product and solution professionals can work with you to understand your company's needs and recommend specific services and optional service features to help your company enhance its fraud prevention posture. Below are just some of the services that we offer:

- **PNC Account Verification Services (AVS)**
A service that can help you confirm critical information regarding the identity and bank account of your intended payees prior to facilitating a payment; helps to reduce fraud losses brought about by imposter fraud scams and administrative costs incurred with returned items.
- **Check Positive Pay**
A service that matches checks presented for payment against your company's check issue file; "exceptions" are presented to you for a pay/return decision through PINACLE, PNC's top-rated corporate online banking platform. PNC offers enhanced Positive Pay service options that include teller line and payee verification.
- **ACH Positive Pay**
A service that allows you to monitor and control ACH debit activity by establishing "rules" that filter the ACH debits coming into your account(s). Using PINACLE, you can review "suspect" ACH debits and determine whether to return them as "unauthorized."
- **ACH Debit Block**
A service that restricts any ACH debit transactions from posting to an account.
- **PINACLE Current Day Information Reporting**
A service that provides intraday information to help you monitor activity within your accounts.
- **PINACLE Event Notifications**
A service that allows you to subscribe to receive notifications about key activities within PINACLE that can be delivered to the PINACLE Message Center, or directly to you via email or text message.
- **IBM Security Trusteer Rapport***
A software application that provides an additional layer of security designed to help protect your login credentials, including your PINACLE Company ID, Operator ID and password.
- **Commercial Card Payments**
An electronic payment option that reduces fraud exposure by allowing you to set spending controls while leveraging transaction monitoring against spending habits that will trigger a fraud alert for suspect transactions.

ENHANCE INTERNAL POLICIES & PROCEDURES

- Store confidential vendor payment information in a secure vendor portal to keep information private and protected.
 - ▶ Know your vendor.
 - ▶ Trust confidential information only with a vendor you have an established relationship with.
 - ▶ As a highly regulated bank, PNC can provide this type of data storage.
- Establish formal policies and procedures for payment processing and accounts payable changes. For example:
 - ▶ Require secondary approval (internally) for all payment requests, payment instruction changes and changes to your accounts payable system.
 - ▶ Require a verbal callout verification process for any vendor payment instruction change request.
 - ▶ Use a third layer (e.g., executive approval) for high-dollar transactions.
- ▶ Set up unique levels of approvals for different payment methods. Wire transfers are final settlements and, as such, may require multi-level approval consideration.
- ▶ Use two- and three-way matching of invoice against an Open PO and Receipt when applicable prior to paying an invoice.
- ▶ Segregate accounts payables system updates and payment initiation functions.
- Review PINACLE security features, controls and operator entitlements:
 - ▶ Confirm that funds movement entitlements are appropriate for each employee's job function.
 - ▶ Segregate payment initiation and payment approval functions.
 - ▶ Implement secondary operator approval of all entitlement changes ("20A") for payment services.

*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.

ADDITIONAL RESOURCES

PNC Security & Privacy

Information and videos about current fraud trends and protocols

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

PINACLE Security Center

Access to important information, updates and tips about how to keep your business safe from cyberfraud

LINK: Click the  icon at the top right of any PINACLE page

PNC Ideas, Insight & Solutions

Articles and 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>

CYBERSECURITY & AWARENESS

QUICK REFERENCE GUIDE

VERIFY AND VALIDATE

- Verify email payment or payment 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 the company 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 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”).

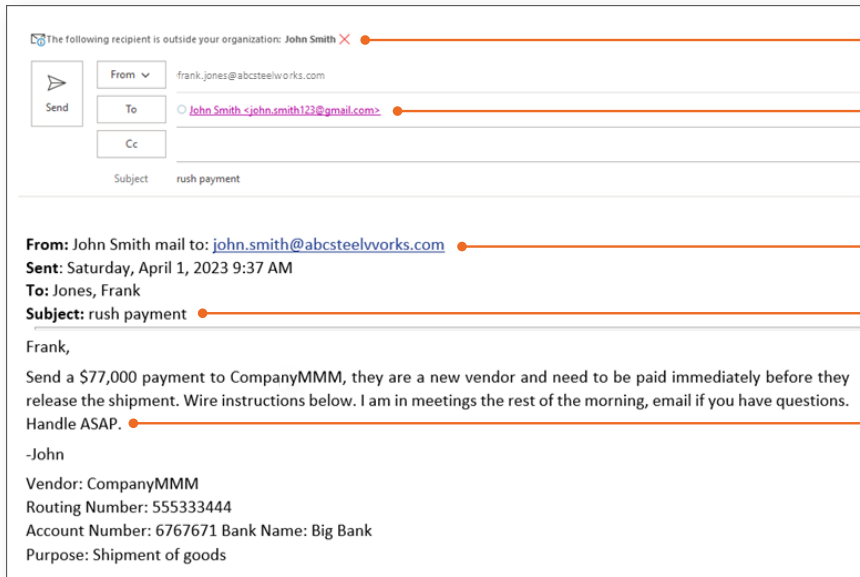
COMMON BEC RED FLAGS

	COMPROMISED INTERNAL EMAIL	COMPROMISED VENDOR EMAIL	FINANCIAL MALWARE	CHECK / WIRE SCAM
Appears to Come from	Company Executive	Existing Vendor	External Business Partner or Vendor	New Customer
Red Flags	<ul style="list-style-type: none"> • Urgent, confidential request • Requestor can be reached only via email 	<ul style="list-style-type: none"> • Requests payment using new account or payment instructions 	<ul style="list-style-type: none"> • Email request to log in to online banking using link provided in the email • Online banking login: <ul style="list-style-type: none"> - Multiple prompts for password/token - Requires second user to log in on same computer 	<ul style="list-style-type: none"> • Overpayment by check or card (non-guaranteed funds) with request for refund via wire transfer (guaranteed funds)
Result	<ul style="list-style-type: none"> • Payment sent to fraudster 	<ul style="list-style-type: none"> • Payment sent to fraudster • Vendor relationship disrupted 	<ul style="list-style-type: none"> • Fraudster obtains login credentials and initiates payment on real bank site 	<ul style="list-style-type: none"> • Company loss of funds reimbursed to fraudster • Check or fraud payment received is invalid

EXAMPLES

EMAIL SPOOFING

Using identity deception tactics like domain or name spoofing, cybercriminals will impersonate a source trusted to their target to trick them into taking a requested action, such as making either a payment or changes to established payment instructions.



Red Flags:

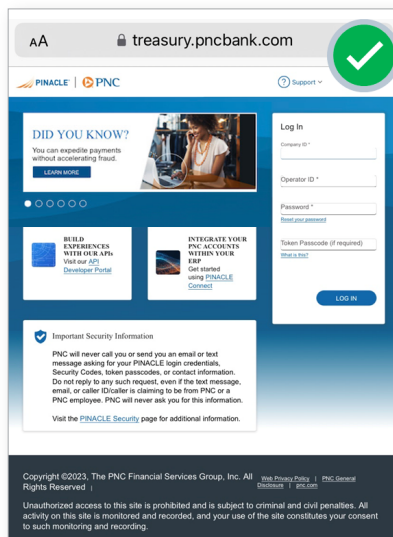
- The following recipient is outside your organization
- When you use "Reply All," the email address appears differently
- The "w" in the company name is spelled with two v's
- It's an urgent request
- The requestor is available only via email

WEBPAGE SPOOFING

Whether through malware infection or domain spoofing, the cybercriminals' ultimate goal is to redirect web traffic away from a legitimate website to a spoofed version of that site. Once on the spoofed site — believing it to be the legitimate site — the target enters their credentials and other sensitive information, attempting to log in to the site. In turn, the cybercriminals use information entered by the target on the spoofed site to log in to the legitimate site, upon which they can gain access to whatever information or tools the target may have.

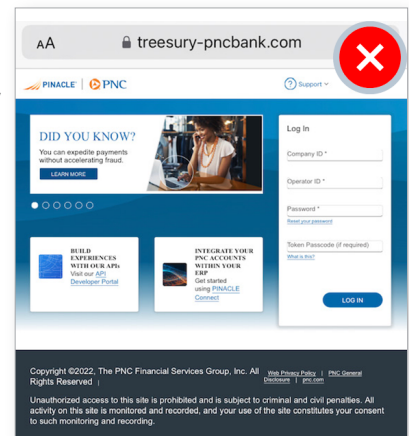
Actual PINACLE login page

We recommend accessing online banking sites like PINACLE with bookmarks or shortcuts as opposed to using a search engine to navigate to those pages.



Spoofed PINACLE login page

- Unrecognized URL
- Omission of the "Important Security Information" box



EXAMPLES

PHISHING

Using email, cybercriminals will send messages containing a link to a malicious website or a malware-infected document attachment to their target. Upon the target's receiving the email and clicking on the link or opening the attachment, unbeknownst to them, the malware will automatically install on their device. In many cases, the malware is designed to redirect web traffic away from a legitimate website to a spoofed version of that site used to harvest login credentials or other sensitive information entered on the site by the cybercriminals' target.

Red Flags:

Message is designed to elicit an emotional response

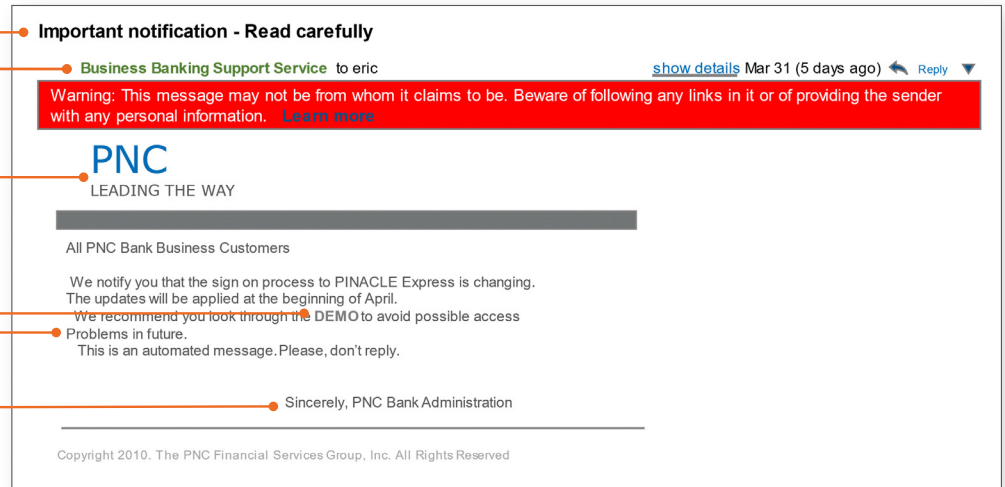
Vague sender name

Improper or incomplete branding

Inclusion of a web link or document attachment

Grammatical and punctuation errors

Formatting or layout anomalies



SMISHING

Similar to phishing, with smishing, cybercriminals will send text messages containing a link to a malicious website or a malware-infected document attachment to their target.

Red Flags:

Unrecognized SMS short code (i.e., sender's phone number)

Improper branding (e.g., "Pinacle" vs. "PINACLE")

Inclusion of a web link or document attachment

Directing to a generic/odd contact for service

<#>PNC Pinacle Alert: ABC Corp. Did you just attempt \$17,550.00 via ACH to [Coinbase.com](#) for bitcoin crypto currency? Reply 1 for yes or reply 2 for no. Any questions call us at the number on the back of your card. Reply STOP to opt out of fraud alerts. Data rates may apply.

DOMAIN SPOOFING

In addition to attempting to install malware to their targets' devices through phishing and smishing scams, cybercriminals may plant spoofed web links on the open web by purchasing advertisements appearing in search engine results page.

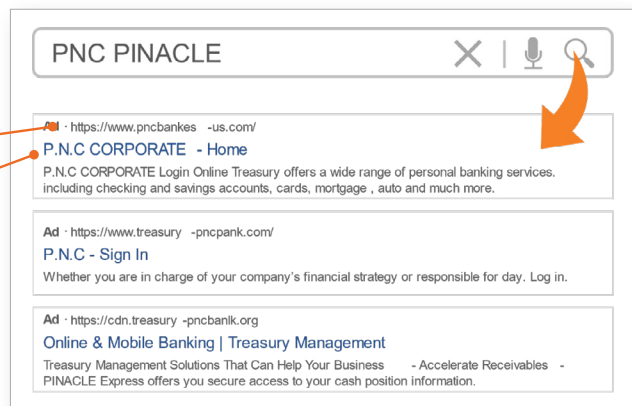
Red Flags:

Unrecognized URL

Improper branding (e.g., "P.N.C" vs. "PNC")

Grammatical and/or punctuation errors

Confusing, illogical and/or nonsensical site description



YOUR CYBERSECURITY CONSIDERATIONS

COMPUTER AND PASSWORDS		✓
⚠ Has your company downloaded Trusteer Rapport malware detection software that is available through PINACLE?		
Does your company require regular password changes every 30 to 90 days?		
Is your company's antivirus software up to date, enabled and set to auto-update?		
Does your company have a dedicated computer for online banking that is not used for email or general internet browsing?		
Does your company utilize any Positive Pay services?		
Does your company use any other fraud surveillance tools or services?		
ENHANCED INTERNAL POLICIES AND PROCEDURES		✓
⚠ Has your executive team reinforced with your payment processing team in writing that all employees, including themselves, must strictly follow the payments processing requirements, policy and procedures?		
Does your organization have formal policies and procedures in place for requesting payments and making additions/changes to your accounts payable system?		
Does your company require secondary approval for all payment requests?		
Does your company require secondary approval for changes to payment instructions in bank and vendor payment systems?		
Does your company require third-layer, executive approval for high-dollar transactions?		
VERIFY AND VALIDATE		✓
⚠ Are email payment or vendor payment change requests confirmed by phone with the vendor using contact information on file (vs. contact information provided in the email request)?		
⚠ Are payment 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 company have a social media policy that employees must read and sign?		
Does your company limit executive contact information on the company website?		
Does your company 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 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 EDUCATION AND AWARENESS		✓
Do all employees with authorization to initiate and approve payment requests receive cybersecurity training?		
Do you provide regular alerts and updated training for employees regarding cyber trends?		
ADDITIONAL RECOMMENDATIONS		✓
<ul style="list-style-type: none"> • Create and manage rules and alerts in PINACLE to monitor and manage time-sensitive activity. • Regularly review user limits and permissions within PINACLE. • Monitor your account for unexpected micro deposits and/or small dollar payments. • Subscribe to Positive Pay service. 		
<p>Once subscribed to Positive Pay:</p> <ul style="list-style-type: none"> • Submit complete, accurate and timely check issue information to the bank for processing. • Log in to PINACLE each business day to review and decision positive pay exceptions. • Reduce your risk of financial loss by setting the positive pay exceptions default decision to "Return." • For enhanced matching and validation, enroll in Payee Positive Pay and Teller Positive Pay. 		



READY TO HELP

If you suspect or experience fraudulent activity, please contact PNC's Treasury Management Client Care immediately at **1-800-669-1518**, Option 1.

Or, if you would like to learn more about protecting yourself from payments fraud, contact your PNC Relationship Manager or Treasury Management Officer.

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.

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

PNC, PNC Bank and PINACLE are registered marks of The PNC Financial Services Group, Inc. ("PNC").

Bank deposit, treasury management and lending products and services, foreign exchange and derivative products (including commodity derivatives), bond accounting and safekeeping services, escrow services, and investment and wealth management and fiduciary services are provided by PNC Bank, National Association ("PNC Bank"), a wholly owned subsidiary of PNC and **Member FDIC**.

Lending, leasing and equity products and services, as well as certain other banking products and services, require credit approval.

©2023 The PNC Financial Services Group, Inc. All rights reserved.

CIB TM PDF 0523-0103-2262802

