



Treasury Management

Cybersecurity Resource Guide

pnc.com/treasury



BRILLIANTLY
BORING
SINCE 1865®



Cyberfraud Overview

Awareness of cyber threats for fraud

Payments fraud attempts are widespread across all industries, driven by business email compromise (BEC), fraudulent texts and phone calls, and financial malware infections meant to steal online banking credentials.

All employees with access to funds movement services must be aware of these types of fraud and be able to 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.



PNC Protect tips

PNC Protect tips highlight simple, actionable steps that help reinforce safe daily behaviors. Look for this icon throughout the guide to identify practical tips designed to help you recognize potential risks and avoid risky situations.



How to use this guide

This resource is designed to help organizations understand today's most common payments fraud threats, recognize warning signs and take practical steps to prevent loss. Use the threat sections to educate your teams, the PNC Protect tips to reinforce daily behaviors, and the Checklist to help assess and strengthen your current controls.

2

Cyberfraud Overview

9

Recommendations and Resources

11

Quick Reference Guide for Employees

17

Cybersecurity Checklist



Attempted fraud via email compromise

There are multiple ways for cybercriminals to initiate fraudulent payment requests or requests to change payment instructions. They can use an email account that appears to be from a customer, vendor or supplier, with a fictitious or cleverly misspelled email address that may or may not match the “From” name of the sender. They can also compromise your customer, vendor or supplier’s actual email address, making it much harder to spot the deception. For those reasons and more, it is essential that your employees recognize the characteristics of a fraudulent payment request.

In many cases, no systems are breached; instead, fraudsters exploit trust, urgency and established business processes to persuade employees to authorize payments.

Many of these attacks result in what is known as authorized push payment (APP) fraud. In these situations, employees authorize a payment believing it to be legitimate, when in fact they have been deceived by a fraudster using impersonation or social engineering techniques. Because the payment is approved by an employee, traditional controls alone may not prevent the loss — making verification and confirmation processes especially important.

Even without compromising an email account, there is a great deal of information available on social media and other public records that cybercriminals can use to perpetrate such schemes. For example, large construction contracts, like those for universities or hospitals, may be disclosed in public filings.



PNC Protect tip

If an email requests new or changed payment instructions, confirm using a known phone number or other trusted method before sending funds, and consider using PNC’s Verification Services solution to help confirm payee identity and bank account details prior to payment.

Cybercriminals can access these records and easily register a website to impersonate a legitimate contractor and contact businesses with “new” accounts and contact information for these projects. Cybercriminals may wait months to initiate contact and use open-source records to identify accounts payable personnel.

Cybercriminals don’t need to know the amount of the upcoming payment or dates for the payment. They can simply say that “All payments going forward should be made to the new account number and to the attention of the new accounts receivable contact.” Victims may be unaware of the fraud until weeks or months have passed, making recovery of funds extremely difficult.



PNC Protect tip

For vendor setup/changes tied to public projects, pair out-of-band verification with payment controls. For example, use **PINACLE Event Notifications** to surface high-risk activity quickly and **Positive Pay** services to help you review and decide exceptions before items are paid.

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

Typical email fraud request scenarios

- A supplier requests changes to payment instructions for an upcoming payment.

Important: Requests to change vendor payment instructions are among the **most common** and **most costly** fraud scenarios and should always be treated as high risk.

- An email appears to be from a company executive to initiate an urgent payment — typically related to 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.



PNC Protect tip

Verify any payment request or change in payment instructions by calling an authorized contact using a phone number from official records (not from the email). This simple step is widely adopted and rated effective for helping prevent BEC.

Recognize the warning signs

- Fraudulent emails typically ask you to 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 often warn of serious repercussions if you don't comply.
- Often, the executive requesting the payment is actually out of the office or unavailable (giving fraudsters more opportunity to misrepresent them).
- Ask yourself:
 - Does this CEO/executive routinely send 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?

In 2025

49%

of fraud via email was made using wire transfers.¹



Take action to help protect against this threat

- Even when emails appear legitimate, compromise can still be in play: **39% of organizations** report they continue to receive **genuine emails that have been intercepted by fraudsters.**¹
- Train your employees to be vigilant when reviewing and confirming payment requests, especially those claiming to be urgent or kept secret.
- 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.
- As fraud tactics evolve, including the use of AI-enabled impersonation, consistent verification and adherence to established controls remain the most effective defenses.



Fraud via phone calls (vishing) and voice impersonation

Fraudsters increasingly call employees — often posing as vendors, customers or even bank representatives — to pressure staff into changing bank details, validating account information or initiating urgent payments. Some schemes use voice impersonation to mimic executives and create credibility.

Recognize the warning signs

- The caller creates urgency (“payment failed,” “past due,” “account will be closed”) and pressures you to bypass normal verification.
- The caller asks you to “confirm” sensitive information (credentials, security codes or account details).
- The caller insists on using a new callback number or refuses standard callback procedures.

In 2025

30%

of organizations reported being targeted by fraudulent phone calls, and 28% received scam texts on company mobile devices.¹



Take action to help protect against this threat

Treat any call asking you to change banking information or use new payment methods as high risk. Hang up and call back using a number from official records or your vendor master file.



PNC Protect tip

Use a “callback” rule: Do not act on inbound payment requests. Instead, initiate a new outbound call using verified contact details and follow normal approval workflows in PINACLE.

Dangerous financial malware infections

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

Once installed on a computer, malware can redirect your online banking session to a malicious site that harvests access credentials such as your User ID, Operator ID, password and security codes.

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



Take action to help protect against this threat

- Verify the authenticity of the communication before opening attachments or clicking on links in any unexpected emails or emails from an unknown sender. Contact the sender at a known telephone number to confirm that the communication was sent by them.
- Use a dedicated computer with no email access and limited internet access for payment initiation or online banking access.

Recognize the warning signs

- 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
 - Repeated prompts to provide your token passcode or security codes, or being presented with a “System Unavailable” message during the login process. **PINACLE will never prompt you to enter login credentials (including a token passcode or security codes) multiple times during the login process.**
 - Being instructed to have a second person enter their login credentials into your computer to initiate a payment, recover a password, log in, etc. **PNC will never ask you to have another PINACLE operator log in to your computer during an online banking session or require another operator to log in to reactivate/unlock an ID.**
 - Sudden issues logging in to PINACLE
 - Subsequently, you may receive a call from someone claiming 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 to resolve the problem.
- Anti-malware software is highly recommended to help strengthen risk mitigation measures against malicious threats.
- PNC offers IBM® Security Trusteer Rapport® as a no-cost, optional risk mitigation tool that can help safeguard your PINACLE login credentials from phishing attempts and to remove certain malware from your computer. Download and install IBM Trusteer by visiting pnc.com/security. To learn more, please visit the PINACLE Security Center.³



PNC Protect tip

Limit PINACLE access to designated devices and users, and use role-based permissions so employees have only the access they need to perform their jobs.

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 post security-procedure updates in advance in the PINACLE Message Center (and you may also receive an email alert if subscribed).

Do not respond to any communication requesting your sensitive information. Report any occurrences to Treasury Management Client Care immediately at 1-800-669-1518, Option 1.

**PNC Protect tip**

If you suspect fraud, time is critical. The sooner you report suspicious activity, the greater the opportunity to help stop additional transactions or attempt recovery of funds.

In the first 60 minutes

- Stop any pending or scheduled payments, if possible.
- Contact Treasury Management Client Care immediately at 1-800-669-1518, Option 1.
- Contact your financial institution immediately and request a recall of the funds (your bank may require additional documentation).
- Preserve emails, instructions and payment details related to the request.
- File a complaint at www.ic3.gov and include full transaction details to support potential fund-freeze efforts.

**Take action to help protect against this threat**

If you experience any of these scenarios or if other 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.





Recommendations and Resources

It's affecting their work

76%

of organizations experienced attempted or actual payments fraud in 2025.¹

58%

of organizations reported attempted or actual payments fraud involving checks in 2025.¹

74%

of organizations were affected by BEC in 2025.¹

Avoid being a statistic

Increase the security of computers and passwords

- Use strong passwords.
- Don't reuse user IDs or passwords.
- Require password changes every 30 to 90 days.
- Confirm antivirus software is current and set to update automatically.
- Install IBM Security Trusteer Rapport malware detection software (see the PINACLE Security Center for details).
- Use dedicated computers for PINACLE access (no email and restricted web access).

Educate employees

- Provide cybersecurity awareness training for employees, contractors and third-party administrators.
- Communicate new cyber trends and alerts.
- Conduct simulated phishing campaigns to test users' ability to recognize phishing emails.

In 2025 IC3 reported

>\$3B

in reported losses from business email compromise (BEC), one of the top cyber-enabled fraud crime types by loss²

>1M

complaints²

>\$20B

in total losses²

Implement fraud solutions

These services can help add checks and alerts around payments so you can spot suspicious activity sooner and reduce the chance of sending funds to the wrong place. Organizations often see the greatest risk reduction by first focusing on payee verification, daily exception review and user access controls, and then layering in additional monitoring and automation.

Verification Services

Helps you confirm counterparty identity and bank account details before you send a payment, reducing imposter-scam losses and the costs of returned payments.

Check Positive Pay

Compares checks presented for payment against the checks you issued; exceptions are presented in PINACLE for your pay/return decision.

ACH Debit Block

Restricts ACH debit transactions from posting to an account.

ACH Positive Pay

Helps you monitor and control ACH debits by setting criteria for which debits can post; suspect items are presented in PINACLE for your review so you can decide whether to return them as unauthorized.

PINACLE Current Day Information Reporting

Provides intraday information to help you monitor activity within your accounts.

PINACLE Event Notifications

Allows you to subscribe to notifications about key activities within PINACLE delivered to the PINACLE Message Center or directly via email or text message.

Commercial Card payments

Reduces fraud exposure by enabling spending controls and leveraging transaction monitoring to flag suspect activity.

Check Print Outsourcing

Provides check printing in a more protected environment using check stock with multiple protection features; check issue information is integrated into Check Positive Pay.

**Customized accounts receivable reporting and UPIC®
(Universal Payment Identification Code)**

A unique account identifier that lets you receive electronic payments without revealing your bank account number.

IBM Security Trusteer Rapport³

Provides an additional layer of safeguards designed to help protect your login credentials, including your PINACLE Company ID, Operator ID and password.

**PNC Protect tip**

ACH Positive Pay can help you monitor and control ACH debits by setting criteria for who can debit your account, with suspect items presented in PINACLE for your review.

Additional resources**PNC Security & Privacy Center**

Information and videos about current fraud trends and protocols

pnc.com/en/security-privacy.html

PINACLE Security Center

Access to important information, updates and tips to help improve your fraud mitigation strategy

**Available in the PINACLE Help
& Training Center****PNC ideas, insights & solutions**

Articles, white papers and insights

pnc.com/insights/cib

FBI Internet Crime Complaint Center

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

www.ic3.gov

www.ftc.gov

www.staysafeonline.org



Cybersecurity and Awareness

Quick Reference Guide

Common business email compromise red flags

	Compromised internal email	Compromised vendor email	Financial malware
Appears to come from	Organization executive	Existing vendor	External business provider or vendor
Red flags	<ul style="list-style-type: none"> Urgent, confidential request Requestor can be reached only via email 	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
Result	Payment sent to fraudster	<ul style="list-style-type: none"> Payment sent to fraudster Vendor relationship disrupted 	Fraudster obtains login credentials and initiates payment on real bank site

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 change in a vendor's 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").

Fraudulent "spoofed" email example

To:	John Smith (john.smith123@gmail.com)
Cc:	
Subject:	rush payment

From: John Smith mail to: john.smith@abcsteelvorks.com
Sent: Monday, October 21, 2026 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

**What's wrong with this picture?**

These images capture some of the ways fraudsters present their scams in ways that seem legitimate. The boxes in this column help point out ways to identify scammers right away.

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 are not currently on file.

Webpage spoofing

Whether through malware infection or domain spoofing, the cybercriminals' goal is to redirect web traffic from a legitimate website to a spoofed version of that site. Once there, you enter your credentials and other sensitive information, attempting to log in to the site. In turn, cybercriminals use your information to log in to the legitimate site, where they gain access to your tools and sensitive information.

The screenshot shows the legitimate PINACLE login page. The browser address bar displays the URL <https://treasury.pncbank.com>. The page features the PNC and PINACLE logos at the top. On the left, there is a 'Did You Know?' section with a 'Learn More' button and a carousel of images. Below this are two promotional boxes: 'Build Experiences With Our APIs' and 'Integrate Your PNC Accounts Within Your ERP'. A prominent 'Important Security Information' box is located below the promotional content, containing text about PNC's security policies and a link to the 'PINACLE Security' page. On the right, the 'Log In' section contains input fields for 'Company ID*', 'User ID*', 'Password*', and 'Token Passcode (if required)'. There are links for 'Reset your password' and 'What is this?', and a 'Log In' button at the bottom.

Actual PINACLE login page

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

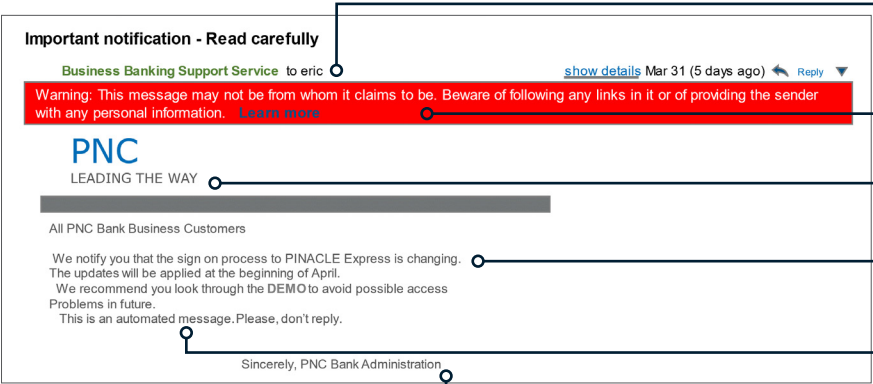
The screenshot shows a spoofed version of the PINACLE login page. The browser address bar displays the URL <https://treasury-pncbank.com>. The page layout is identical to the actual page, but it is missing the 'Important Security Information' box. The 'Log In' section on the right is identical to the actual page, with input fields for 'Company ID*', 'User ID*', 'Password*', and 'Token Passcode (if required)', and links for 'Reset your password' and 'What is this?'. The 'Log In' button is at the bottom.

Spoofed PINACLE login page

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

Phishing

Using email, cybercriminals will send messages containing a link to a malicious website or a malware-infected attachment. When you receive the email and click on the link or open the attachment, the malware will secretly be installed on your device. In many cases, the malware may redirect web traffic away to a spoofed website to harvest your login credentials or other sensitive information.



Message is designed to elicit an emotional response

Vague sender name

Improper or incomplete branding

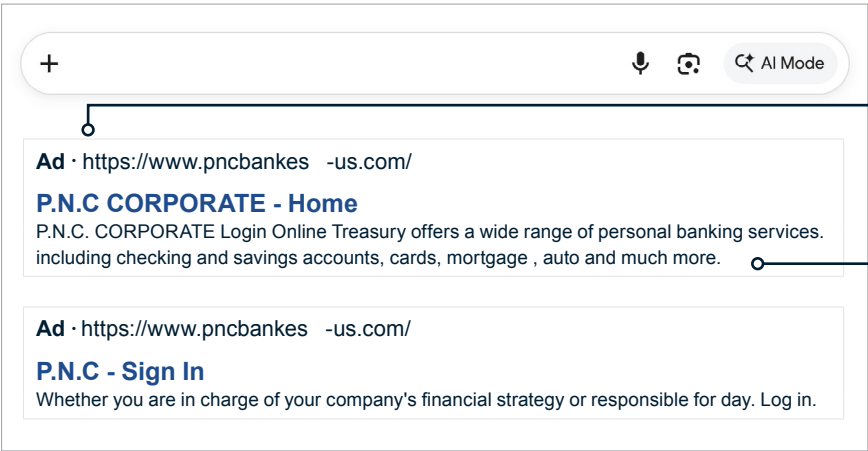
Inclusion of a web link or document attachment

Grammatical and punctuation errors

Formatting or layout anomalies

Domain spoofing

Cybercriminals plant spoofed web links by purchasing advertisements in search engine results and direct users to look-alike sites designed to harvest credentials.



Unrecognized URL

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

Grammatical and/or punctuation errors

Confusing, illogical and/or nonsensical site description



PNC Protect tip

Always access PINACLE by using a saved bookmark or by typing the known web address directly into your browser, never through links in emails, texts or even search engine hits.

Smishing

Like phishing, smishing uses text messages that include a link to a malicious website or a malware-infected document attachment. In 2025, **92% of organizations** reported receiving **spoofed text messages** on company phones, and **11% reported fraudulent QR codes**.¹



PNC Protect tip

PNC will never ask you to click a link or share login credentials by text. If a message appears to be urgent, sign in to PINACLE directly or contact Treasury Management Client Care to verify.

PnC Online Banking Alert: ABC Corp.

Did you just attempt \$17,550.00 via ACH to [Crypto.com](#) for bitcoin crypto currency?

Reply 1 for yes or reply 2 for no.

Any questions call us at [\(888\) 762-2265](#).

Reply STOP to opt out of fraud alerts. Data rates may apply.

PNC alert! A pending charge of \$1,320 to Acme Corp.

Not aware? Cancel debit request here: <https://pncweb.click/visit/>

Short code
(i.e., sender's phone number)

Improper branding
(e.g., "PnC" vs. "PNC")

Inclusion of a web link or document attachment directing to a generic/odd contact for service



Additional recommendations

- 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 services.



PNC Protect tip

Use Check Positive Pay to compare checks presented for payment against the checks you issued and review exceptions in PINACLE so you can decide which items should be paid or returned.

Once subscribed to Positive Pay:

- 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.
- Help reduce your risk of financial loss by setting the positive pay exceptions default decision to “Return.”

Add PNC’s short codes to your contacts to help identify and avoid engaging with smishing attempts:

PINACLE Security — 76200

You will receive Security Codes from this short code when logging in to PINACLE or updating your PINACLE user profile information.

PINACLE Event Notifications — 762242

You will receive Event Notifications from this short code if you subscribe to SMS delivery. Notifications may include authentication-related actions, balance and transaction details, payment approvals, payment status changes and Positive Pay exceptions.

Commercial Card — 762411

You will receive messages from this short code for Commercial Card information. Messages may include next payment due, payment made, declined transactions and daily balance activity as well as fraud alerts asking for confirmation regarding a specific card transaction.

ePayments — 26489

Your Payees will receive notifications and reminders to facilitate payment selection based on your payment instructions.



Cybersecurity Checklist

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 payment 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/third-party 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?

Let's build your brilliant.



If you suspect or experience fraudulent activity, please contact PNC's Treasury Management Care Center 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.

¹ Association for Financial Professionals (AFP), 2026 AFP® Payments Fraud and Control Survey Report: Key Highlights (April 2026) — results reported for 2025.

² Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), 2025 IC3 Annual Report.

³ Trusteer is a third party, 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.

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. UPIC is a registered trademark of The Clearing House Payments Company, LLC.

PNC, PNC Bank, PINACLE, and Brilliantly Boring since 1865 are registered marks of The PNC Financial Services Group, Inc. ("PNC").

Bank deposit, treasury management and lending products and services, foreign exchange, derivatives products, 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.

©2026 The PNC Financial Services Group, Inc. All rights reserved.

CIB TM PDF 0626-018-1540144