

# Mid Council Financial Network Conference Payment Fraud Controls

November 7-9-, 2018



- **Terminology**
- **How big of an issue is fraud?**
- **Fraud risks affecting ALL businesses, including churches**
  - Fraudulent Checks
  - Business Email Compromise
  - Card Fraud
  - Malware
  - Account Takeovers
  - Electronic Payment Portal Risks
- **Fraud prevention strategies and training**



### ▪ **Malware**

- Malicious software downloaded to a PC or mobile device; used to capture keystrokes, exploit system vulnerabilities, steal information, etc.



### ▪ **Social Engineering**

- Manipulating people into performing actions or divulging confidential information



### ▪ **Phishing**

- Emails used to gather information or deliver malware (through infected attachments or links to malicious sites)



### ▪ **Smishing**

- Text messages used to gather information or infect the mobile device

# The Stark Reality of Today's Payment Channel Fraud Threats



**78%**

Organizations experiencing actual or attempted payments fraud in 2017



**54%**

Organizations experiencing actual losses from business email compromise in 2017



**3/4**

Payment fraud ratio that is check based



**30%**

Organizations that were subject to ACH debit fraud

**\$676,000,000**

15,700 BEC complaints in 2017 to the FBI IC3 (Internet Crime Complaint Center)

Sources:  
2018 Association for Financial Professionals Payments Fraud and Control Survey  
2017 FBI Internet Crime Report

# Fraud Risks in Payments

## Types of Risks



Type of Fraud Risk	Payment Channel(s)
<b>Fraudulent Checks</b>	Checks
<b>Business Email Compromise</b>	Typically Wire Transfer
<b>Card Fraud</b>	Credit & Debit Cards
<b>Malware</b>	Not payment-channel specific
<b>Account Takeovers</b>	Any
<b>Electronic Payment Portal Risks</b>	ACH or Card

# Fraudulent Checks

Checks debiting your church accounts

### Positive Pay

- Church / Organization provides PNC with a transmission of **check issue data**
- PNC matches checks presented for payment against check issues received and **reports any exception items each day** (incl. check images)
- Exceptions are presented by 11:00 a.m. ET with client decisioning required by 3:00 p.m. ET via PINACLE® Positive Pay Module
- **Payee Positive Pay** with **Teller Positive Pay** are additional optional services

### Reverse Positive Pay

- PNC provides clients with **daily paid check data** via files, PINACLE®
- Clients can **compare check data to their internal check issue database** to identify any mismatched items

Exceptions												
Decisions submitted after 03:00 PM ET will not be accepted.												
Account: 9914827961 [Payables A] <input type="button" value="Search"/>												
Account Number	Serial Number	Issue Date	Issue Amount	Paid Date	Paid Amount	Add'l Data	Payee Name 1	Payee Name 2	Exception Description	Account Default	Action	Exception Decision
9914827961	<a href="#">2013</a>	10/21/2007	\$20.00	10/21/2007	\$20.00	Addition al Data	ABC Groomers1	ABC Groomers2	ACH Converted Check - Payee Mismatch	RET	Exception	<input type="button" value="v"/>
9914827961	<a href="#">2012</a>	10/21/2007	\$5,623.00	10/21/2007	\$5,623.00	Pitts Pi zza Pal	Pittsburgh Pizza Palace	Downtown Location	ACH Converted Check - Payee Mismatch	RET	Exception	<input type="button" value="v"/>
9914827961	<a href="#">2000</a>	10/21/2007	\$20.00	10/21/2007	\$20.00	Addition al Data	ABC Groomers1	ABC Groomers2	Payee Not Available	PAY	Exception	<input type="button" value="v"/>
9914827961	<a href="#">2011</a>	03/14/2006	\$289.00	03/15/2006	\$289,000,000.00				Paid Amount Does Not Match Issue	RET	Exception	<input type="button" value="v"/>
9914827961	<a href="#">1050</a>	03/01/2006	\$3,201.00	05/18/2011	\$3,201.00				Payee Not	PAY	Exception	<input type="button" value="v"/>

# Business Email Compromise

Requests for fraudulent funds movement



- **BEC – Business Email Compromise**

- Also known as: Executive Impersonation & Vendor Impersonation – “**Imposter Fraud**”

- **Hacked or spoofed (fictitious) email accounts are used to request:**

- **Urgent / important** payments (typically wire transfer)
- Changes to established **payment instructions** for a supplier
- Employee W2 information (typically seen during tax season)

- **Requests impersonate a known or trusted source:**

- Company or organization executive
- Supplier or vendor



# Spoofer Email Accounts

## What to look for



- **An email domain that is a legitimate-appearing variation of your official email domain (or your trading partner's official domain):**

- pnc-corp.com vs. pnc.com
- steelcityco.com vs. steelcitycorp.com

- **An email domain that mimics the legitimate one using visual tricks:**

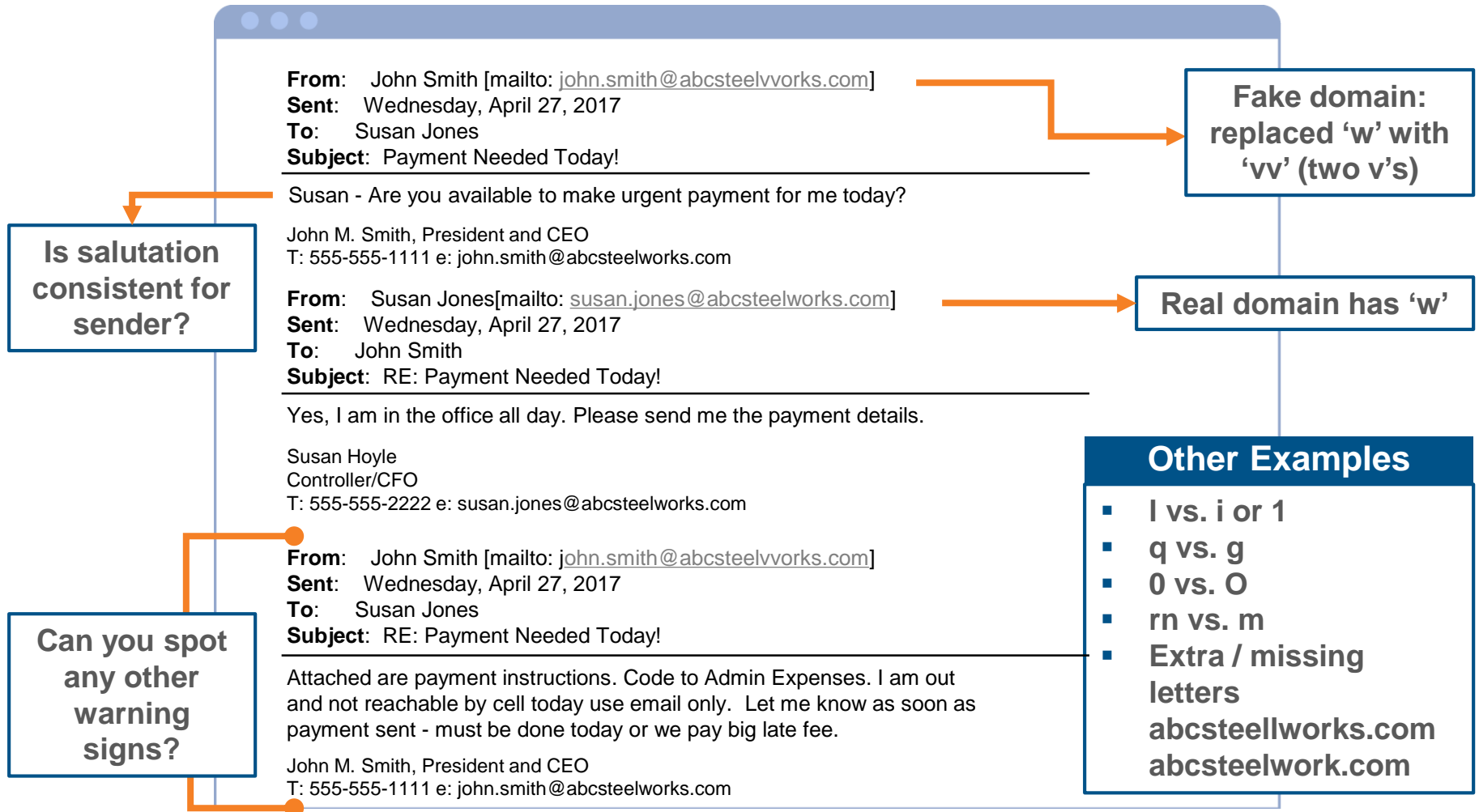
- lovves.com
- hornedepot.com

- **Protection Strategies Against Domain Spoofing:**



- 1 – Register Your Organization Domain Name Variations
- 2 – Create Email Rules to Identify Emails from External Sources

# An Example of a Domain Name Spoof





- **The (criminal) requestor typically:**
  - Insists on secrecy or confidentiality (e.g., payment is for an acquisition or investment)
  - Suggests “generic” accounting for the payment
  - Warns of negative consequences for failure to comply with the request
  - Insists on communication via email
  - Wants immediate confirmation when the payment is executed
  
- **Email Salutation / Closing:**
  - How is the email addressed and signed, compared to what is typical for the sender?
  - (e.g., “Dear Suzanne” vs. “Hi Sue” or “Bob” vs. “Robert”)

3

## ▪ Establish Policies and Procedures for Payment and Vendor Management Processes

- Require secondary approval (internally) for all payment requests and payment instruction changes in bank and ERP systems
- Require independent verification with any requestor to confirm email payment requests or payment account number changes
  - Verification should be via direct contact with a known individual; do not use email to verify the request
- Ensure that organization executives support and agree to follow established procedures

4

## ▪ Educate and Empower Employees

- Train employees to recognize the warning signs of email compromise
- Empower employees to question suspicious emails or payment requests appearing to be from organization executives

5

## ▪ Protect Your Receivables

- Establish a process for providing electronic payment instruction changes to your customers
- Communicate the process as you onboard new customers so they know what to expect



- **How criminals create compelling and realistic sounding emails:**
  - View publically available information (Internet)
  - Scan social networking sites
  - Send spam email to look for out of office replies
  - Review a compromised executive's / supplier's legitimate mail account
    - Gather facts about the business and upcoming payments
  
- **Additional protection strategies:**
  - Ensure employees practice smart social media habits
  - Do not send 'Out of Office' replies externally
  - Require independent verification of all email payment requests

# Card Fraud

Online and in-person card fraud risks

### ▪ Description:

- Transactions that the cardholder or authorized user claim are unauthorized
- Account number no longer in use or is fictitious, or
- The merchant was identified as “High Risk” due to excessive fraud



#### Reason Codes & Description

- 57 – Fraudulent Multiple Transactions
- 62 – Counterfeit Transaction\*
- 81 – Fraudulent Transaction – Card-Present Environment
- 83 – Fraudulent Transaction – Card-Not Present Environment
- 93 – Merchant Fraud Performance Program

#### Reason Codes & Description

- 37 – No Cardholder Authorization
- 40 – Fraudulent Processing of Transactions
- 49 – Questionable Merchant Activity
- 63 – Cardholder Does Not Recognize Potential Fraud
- 70 – Chip Liability Shift\*
- 71 – Chip/PIN Liability Shift\*

\*Designates EMV Reason code



### How to Avoid Fraud Disputes

- If card is **chip-enabled**, dip card into POS terminal.
- Dip card whenever possible, if unable to dip ensure **proper fallback swipe** or key entered
- If magnetic swipe fails, perform a **valid imprint** of the card using the proper device.
- Ensure **merchant descriptor** matches the name of the business and is displayed correctly on cardholder statements.
- Implement point-of-sale and internal fraud prevention policies.
- **Retain permitted consumer data** for research purposes or to allow contact when applicable.
- Utilize alternative account verification sources (e.g. negative databases, fraud screening tools, account updater, or other means to validate the cardholder's identity).

### How to Defend Fraud Disputes

- Provide a **signed, imprinted or electronically captured** copy of the transaction document.
- Provide a **written letter of acceptance from the cardholder**
- Follow other instructions provided on the Chargeback Notice.
- Respond with documentation showing a positive Verified by Visa or MasterCard SecureCode response.
- If this information is not available, you may have to work directly with the cardholder to resolve the dispute.
- Provide compelling evidence to support charge. (Not true remedy)

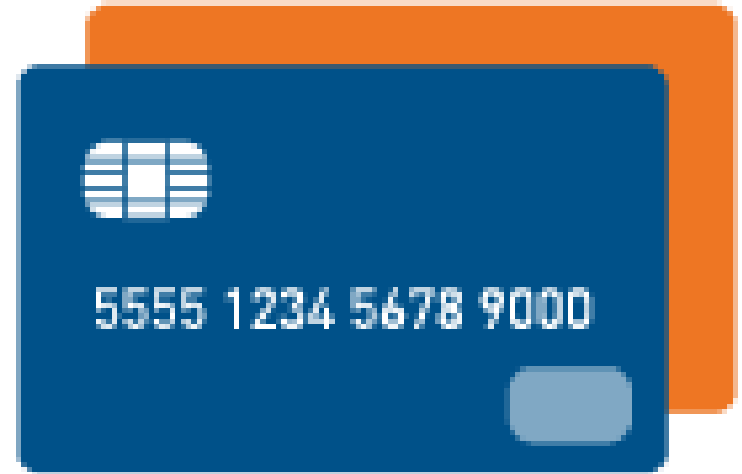
- **Terminal transactions**

- EMV enabled  
(otherwise, liability shift)
- Confirming cardholder or business name

- **Vendor due diligence**

- **Online transactions**

- Annual PCI Compliance certifications for internal process
- Assess PCI Compliance of vendors that support on-line purchases, contributions and payments



# Malware

Software execution from E-Mail or Website links that infects your network

## How Do I Get It?

- Malware may be embedded in **phishing emails** via infected attachments or a link that, when clicked, **infects the computer and possibly whole network** with malware

## How Does It Function?

- When trying to log in to **online banking**, you are directed to a **login page that looks just like the bank's page** where the fraudster captures your login credentials
- Fraudster then **uses your login credentials**

## What Are Red Flags?

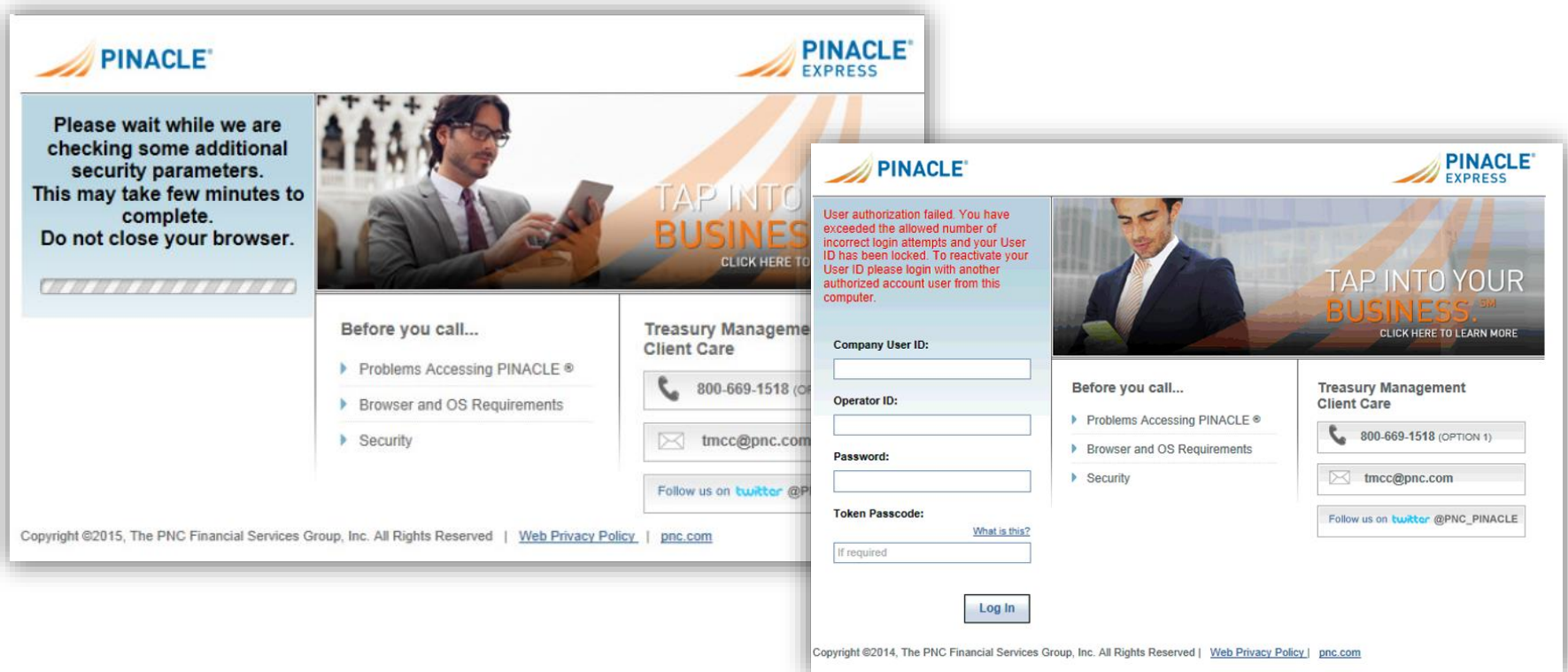
- **Stalled screens and prompts** for login information that are outside of the typical workflow
- Prompt to **log in as a second user** from the same computer

## Best Practices

- Do not open **attachments** or click on **links** in emails from **unknown senders**
- **Install FREE** IBM® Security Trusteer Rapport® malware detection software
- Ensure PINACLE® **Operator entitlements** are appropriate for an individual's job responsibilities
- Use **Secondary Operator Approval** ("2OA") for PINACLE entitlement changes
- Subscribe to **PINACLE Event Notifications** for account activity and payments pending approval
- Call TM Client Care at 800-669-1518, option 1 if you are **having difficulty logging in** or receive **unusual error messages**

# Examples of How Financial Malware Works

- The criminals use the fraudulent site to deliver additional authentication prompts and “stall screens” to the user
- Once the criminals successfully create a payment, they will use the fraudulent site to gain access to a second set of credentials for payment approval



**Left Screenshot (Stall Screen):**

**PINACLE EXPRESS**

Please wait while we are checking some additional security parameters. This may take few minutes to complete. Do not close your browser.

**TAP INTO YOUR BUSINESS**  
CLICK HERE TO LEARN MORE

**Before you call...**

- ▶ Problems Accessing PINACLE
- ▶ Browser and OS Requirements
- ▶ Security

**Treasury Management Client Care**

800-669-1518 (OPTION 1)

tmcc@pnc.com

Follow us on [twitter](#) @PNC\_PINACLE

Copyright ©2015, The PNC Financial Services Group, Inc. All Rights Reserved | [Web Privacy Policy](#) | [pnc.com](#)

**Right Screenshot (Error Screen):**

**PINACLE EXPRESS**

User authorization failed. You have exceeded the allowed number of incorrect login attempts and your User ID has been locked. To reactivate your User ID please login with another authorized account user from this computer.

**TAP INTO YOUR BUSINESS**  
CLICK HERE TO LEARN MORE

**Before you call...**

- ▶ Problems Accessing PINACLE
- ▶ Browser and OS Requirements
- ▶ Security

**Treasury Management Client Care**

800-669-1518 (OPTION 1)

tmcc@pnc.com

Follow us on [twitter](#) @PNC\_PINACLE

Copyright ©2014, The PNC Financial Services Group, Inc. All Rights Reserved | [Web Privacy Policy](#) | [pnc.com](#)

# Online Banking Security Information



**PINACLE | PNC** Home My Profile Message Center Administration Contact Us Quick Links Help & Training Log Out

A/R ADVANTAGE DEPOSIT ON-SITE INFORMATION REPORTING ACCOUNT ANALYSIS STATEMENTS ACCOUNT TRANSFER ACH CORPORATE CARD ACH POSITIVE PAY ARP STATEMENTS CASH LOGISTICS MA

**You have 2 Alerts in the Message Center**

Welcome, Blaine Carnprobst  
PINACLE WEB TEST

Thursday, October 25, 2018  
Last Successful Login: Wednesday, October 24, 2018 at 2:51PM EDT

**TAP INTO YOUR BUSINESS.**

#### Information Reporting Favorites

★ <a href="#">Balance</a>	CSV	Print
★ <a href="#">Cash Position</a>	CSV	Print
★ <a href="#">Debit and Credit Adjustments</a>	CSV	Print
★ <a href="#">Summary and Detail</a>	CSV	Print
★ <a href="#">Summary and Detail</a>	CSV	Print

#### Message Center

##### Alerts

System Alerts	0
Security Messages	0
Informational Messages	1
Product Enhancements	1

#### My Contacts

Treasury Management Client Care 800-669-1518

Name	Phone
<a href="#">+ Add Contact</a>	
<b>Mike Smith</b> mike.smith@gmail.com	412 234 100

#### PINACLE News

**NEW** [Enhanced ACH Positive Pay and Payables Advantage Admin Functions](#)  
ACH Positive Pay and Payables Advantage have been converted to the new 'Administration' module. *Posted 10/15/2018*

#### Information Reporting Balances

Current Day Previous Day

As of Date: Thursday, October 25, 2018

Select an account to review details.

#### Did You Know...

**Quick Links**

- Add Issue Data
- Canada Express

that you can easily navigate to the most commonly used PINACLE

PINACLE | PNC

Home My Profile Message Center Administration Contact Us Quick Links Help & Training Log Out

A/R ADVANTAGE DEPOSIT ON-SITE INFORMATION REPORTING ACCOUNT ANALYSIS STATEMENTS ACCOUNT TRANSFER ACH CORPORATE CARD ACH POSITIVE PAY ARP STATEMENTS CASH LOGISTICS MAINTENANCE

You have 2 Alerts in the Message Center

## Security Center

PNC values the safety and security of your PINACLE login credentials and financial information, and we have implemented a comprehensive suite of security controls to address the increasing volume and sophistication of online banking cyber-threats. The Security Center contains various documents to assist you in maintaining the security and confidentiality of your information, including the latest PINACLE Security Features and Controls as well as educational information regarding security best practices and potential security threats. Additionally, the Security Center's Business Resiliency panel includes forms for providing payment instructions to PNC via alternative methods when access to PINACLE services is not available, as well as a best practices document to help you prepare for a business interruption. Please familiarize yourself with this information and contact PNC's Treasury Management Client Care group or your Treasury Management Officer if you have any questions.

PINACLE | PNC Security

Business Resiliency

Resources and Tools

Alerts

Security practices and prevention methods raise the level of protection against fraudulent activity. Familiarize yourself with both required and optional controls when developing your own "Security Procedure."

[Security Features and Application Controls](#)

[Online Best Practice Controls](#)

**UPDATE** [Mobile Security Features](#)

[Reporting Fraud](#)

Be prepared for events that may affect your primary online access and processes with the bank.

[Business Resiliency Best Practices](#)

[Funds Transfer Business Resiliency Form](#)

Stay informed regarding security trends, recommendations and available services.

[Ransomware](#)

[Trusteer Rapport FAQs](#)

[Third-party Security Sites](#)

[Examples of Phishing Emails](#)

[ARP Positive Pay and Payee Matching](#)

Review information about Security Messages posted in the PINACLE Message Center in a timely manner and react accordingly to protect yourself from fraudulent activity.

[Welcome to the Security Center!](#)

[Attempted Wire Fraud via Email Requests](#)

[Financial Malware Reported](#)

## ▪ Defined

- Theft of your **online banking credentials** to initiate and approve payments
- Typically involves **sophisticated financial malware** that deploys keystroke loggers, site redirects, page injections
- Malware downloads **from infected email attachment or malicious website**

## 1 ▪ Protection Strategies Against Account Takeover

- Require **Dual Approval** for Payments With All of Your Banking Partners

## 2 ▪ Educate Employees (*Recurring Theme!*)

- Know the **warning signs** of an account takeover
- Ensure users are familiar with “**normal**” online authentication workflows
- Enforce cyber best practices (**do not click on links or open attachments** in emails from unrecognized senders)

## 3 ▪ Use Malware Protection Software

- (e.g., IBM Security Trusteer Rapport)c



# Electronic Payment Portal Risks

# What risks do you need to be aware of with a service like PayerExpress?

---

- **Enrolled church members are adding their personal bank account information and possibly credit cards**
  - Stored on **secure servers** through PNC that are PCI, HIPAA and HITECH compliant
- **Debits to invalid bank accounts**
  - Members enrolling are providing bank account information and **recurring contributions**
  - **Not likely** that a member would set up an invalid account number (other than data entry error)
- **Funding credits to churches misdirected to invalid recipients**
  - Fund receipt organization is **coded** into a PayerExpress implementation
  - This **cannot be changed by any users** in the system (even a church employee)

# Fraud Risks in Payments

## Recap of Types of Risks & Mitigants

Type of Fraud Risk	Payment Channel(s)	Fraud Mitigants
<b>Fraudulent Checks</b>	Checks	<ul style="list-style-type: none"> <li>• Positive Pay</li> <li>• Control of Check Stock</li> <li>• MICR printing “on the fly”</li> <li>• Check-print outsourcing</li> </ul>
<b>Business Email Compromise</b>	Typically Wire Transfer	<ul style="list-style-type: none"> <li>• “External” alerts on inbound emails</li> <li>• Employee training &amp; testing</li> <li>• Phishing alert button or reporting tool</li> <li>• Dual-control to execute and approve Wires</li> </ul>
<b>Card Fraud</b>	Credit & Debit Cards	<ul style="list-style-type: none"> <li>• EMV readers at POS</li> <li>• Fraudsters going to path of least resistance</li> <li>• PCI compliance reviews and certification</li> <li>• Internal procedures for handling of card transactions, particularly any documents containing card numbers</li> </ul>
<b>Malware</b>	Not payment-channel specific	<ul style="list-style-type: none"> <li>• Employee training &amp; testing – DON'T CLICK LINKS</li> <li>• Software blocks of external files, particularly ZIP &amp; EXE files</li> </ul>
<b>Account Takeovers</b>	Any	<ul style="list-style-type: none"> <li>• Recognize standard bank account access procedures</li> <li>• Do NOT click email links that appear to be from the bank instructing you to log into your account</li> <li>• Monitor all transaction activity and promptly notify the bank if you suspect fraud</li> </ul>
<b>Electronic Payment Portal Risks</b>	ACH or Card	<ul style="list-style-type: none"> <li>• Utilize EMV-enabled terminals in any “card present” environment</li> <li>• Ensure vendor compliance with PCI for any online systems utilized for your member donations and payments</li> </ul>

## ▪ Essential Components of Employee Education and Training Programs

- Ensure all employees know how to **recognize phishing attempts**
- Conduct **periodic phishing assessments** to know where to focus future education and training
- Ensure employees understand the importance of having smart **social media habits**
- Provide additional education about **recognizing BEC schemes** and the actions of malware to church staff



## ▪ 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

## ▪ Information Protection

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

## ▪ Business Email Compromise (BEC) Detections

- Inspect email header and look for **alterations** (e.g., use of two “Vs” 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 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”)

- **Awareness**
  - Endorsed by Executive Leadership
  - Educate your staff
  
- **Prevention**
  - Define and implement a preventative approach
  - It is better to prevent than to attempt to recover
  
- **Assessment**
  - Regular evaluation and updating of plan
  - Fraudsters are doing this: 399 out of 400
  
- **Detection**
  - Use technology, process and intuition to identify a fraud event
  
- **Response**
  - Plan for your response: Time is of the essence
  - Notification: Across > Up > Out

PNC, PNC Bank, ACHIEVEMENT, PINACLE, Working Cash, ActivePay, Global Trade Excellence, Vested Interest, Midland Loan Services, Enterprise!, CMBS Investor Insight, Portfolio Investor Insight, Borrower Insight, Shared Servicing, PNC Riverarch Capital, and PNC Erieview Capital are registered marks of The PNC Financial Services Group, Inc. (“PNC”). PNC Retirement Solutions is a service mark of PNC.

Bank deposit, treasury management and lending products and 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. Certain fiduciary and agency services are provided by PNC Delaware Trust Company. Foreign exchange and derivative products (including commodity derivatives) are obligations of PNC Bank. Equipment financing and leasing products are provided by PNC Equipment Finance, LLC, a wholly-owned subsidiary of PNC Bank. Energy financing is provided by PNC Energy Capital LLC, a wholly-owned subsidiary of PNC Equipment Finance, LLC. Aircraft financing is provided by PNC Aviation Finance, a division of PNC Equipment Finance, LLC. Asset-based lending is provided by PNC Business Credit, a division of PNC Bank and PNC Financial Services UK Ltd. (an indirect wholly-owned subsidiary of PNC Bank) in the United Kingdom. Specialty finance products are provided by Steel City Capital Funding, a division of PNC Bank. Merchant services are provided by PNC Merchant Services Company. Direct equity investing and mezzanine financing are conducted by PNC Capital Finance, LLC through its PNC Riverarch Capital, PNC Mezzanine Capital and PNC Erieview Capital divisions. Investment banking and capital markets activities are conducted by PNC through its subsidiaries PNC Bank, PNC Capital Markets LLC, Harris Williams LLC, Harris Williams & Co Ltd. and Solebury Capital LLC. Services such as public finance investment banking services, securities underwriting, and securities sales and trading are provided by PNC Capital Markets LLC. Merger and acquisition advisory and related services are provided by Harris Williams LLC and Harris Williams & Co. Ltd. Equity capital markets advisory and related services are provided by Solebury Capital LLC. PNC Capital Markets LLC, Harris Williams LLC and Solebury Capital LLC are registered broker-dealers and members of FINRA and SIPC, and Harris Williams & Co. Ltd is authorized and regulated by Financial Services Authority (FRN No. 540892). Harris Williams & Co is the trade name under which Harris Williams LLC and Harris Williams & Co. Ltd. conduct business. Retail brokerage services and managed account advisory services are offered by PNC Investments LLC, a registered broker-dealer and a registered investment adviser and member of FINRA and SIPC. Annuities and other insurance products are offered through PNC Insurance Services, LLC. PNC Bank is not registered as a municipal advisor under the Dodd-Frank Wall Street Reform and Consumer Protection Act (“Act”). Investment management and related products and services provided to a “municipal entity” or “obligated person” regarding “proceeds of municipal securities” (as such terms are defined in the Act) will be provided by PNC Capital Advisors, LLC, a wholly-owned subsidiary of PNC Bank. PNC Bank and certain of its affiliates including PNC TC, LLC, an SEC registered investment advisor wholly-owned by PNC Bank, do business as PNC Real Estate. PNC Real Estate provides commercial real estate financing and related services. Through its Tax Credit Capital segment, PNC Real Estate provides lending services, equity investments and equity investment services relating to low income housing tax credit (“LIHTC”) and preservation investments. PNC TC, LLC provides investment advisory services to funds sponsored by PNC Real Estate for LIHTC and preservation investments. Registration with the SEC does not imply a certain level of skill or training. This material does not constitute an offer to sell or a solicitation of an offer to buy any investment product. Risks of each fund are described in the funds’ private placement memorandum or other offering documents.

**Important Investor Information: Securities and insurance products are:**

**Not FDIC Insured • Not Bank Guaranteed • Not A Deposit  
Not Insured By Any Federal Government Agency • May Lose Value**

In Canada, PNC Bank Canada Branch, the Canadian branch of PNC Bank, provides bank deposit, treasury management, lending (including asset-based lending through its Business Credit division) and leasing and lending products and services (through its Equipment Finance division). Deposits with PNC Bank Canada Branch are not insured by the Canada Deposit Insurance Corporation. Deposits with PNC Bank Canada Branch are not insured by the Federal Deposit Insurance Corporation, nor are they guaranteed by the United States Government or any agency thereof. In the event of the failure of PNC Bank, deposits with PNC Bank Canada Branch would be treated as unsecured general liabilities, and creditors would be considered general creditors of PNC Bank.

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

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 does not provide investment advice to PNC Retirement Solutions and Vested Interest plan sponsors or participants.

©2018 The PNC Financial Services Group, Inc. All rights reserved.

