Risk Mitigation for Originators: Considerations for Reducing Risk in Payments Processing

Utility Payment Conference 2018

NACHA
The Electronic Payments Association®

Reducing Payment Risk

Overall objective: ensuring good payment

- Applies across all payment methods
  - ACH
  - Wire
  - Check
  - Cashiers' check, etc.
- Applies to all payers and receivers
  - Governments
  - Businesses
  - Consumers

Reducing Payment Risk

Keys to ensuring good payment

- Proper authorization
- Proper authentication
- Broad fraud protections

Reducing Payment Risk

Proper authorization

- Clear and conspicuous
- Complete terms
- Recognizable as an authorization
- In accordance with payment system requirements

Reducing Payment Risk

Proper authentication

- Name on authorization corresponds to a real person
- Real person has privileges on the account in the authorization
- Commercially reasonable methods

Protecting Against Fraud

Cyber-enabled financial fraud

- Also known as Business Email Compromise (BEC)
- Fraudsters moving from malware to BEC
  - Easier to execute due to social media
- Fraudsters are
  - Adept at running a business
  - Neutral as to payment methods

Protecting Against Fraud

Cyber-Enabled Financial Fraud Pattern

1. Targeting
2. Grooming
3. Exchange of information
4. Execution of fraudulent transaction

Cyber-Enabled Financial Fraud

- Not limited to email
- Various types of cyber-enabled financial fraud schemes
  - Business Email Compromise
  - Vendor Impersonation Fraud
  - Payroll Impersonation Fraud
- General prevention
  - Employee awareness
  - Employee vigilance
  - Dual controls for payments

Business Email Compromise

What is it?

- Legitimate business email accounts are either compromised or impersonated
- Email account usually belongs to an officer of the business

Business Email Compromise

How is it done? The fraudster

1. Monitors officer's accounts for information
2. Gains access to or impersonates the email account
3. Uses the compromised email account to send payment instructions
4. Directs payment to an account controlled by the fraudster

Business Email Compromise

Prevention

- Authenticate requests to make payments or change payment information
- Be mindful of information provided on social media
- Consider registering domains that closely resemble the company's actual domain
  - abc_inc.com vs. abc-inc.com
- Don't use "reply" when authenticating payment request emails. Use "forward" and type in the correct email address

Vendor Impersonation Fraud

What is it?

- A business receives an unsolicited request, purportedly from a valid contractor, to update payment information for the contractor
  - Account information
  - Payment method
- Public sector entities targeted more often
  - Contracting information is frequently public

Vendor Impersonation Fraud

How is it done? The fraudster

1. Monitors target entity for publicly available contracting or vendor information
2. Contacts the entity posing as legitimate vendor to change payment information to an account controlled by the fraudster
3. Requests payment to the fraudster's account

Vendor Impersonation Fraud

Prevention

- Make vendor payment forms available only via secure means or to known entities
- Require changes to payment account information to be made or confirmed by site administrators
- Use methods like verification codes to existing contacts
- Do not ignore calls from your financial institution questioning an outgoing payment

Payroll Impersonation Fraud

What is it?

- Employees directed to update or confirm payroll information via a fake payroll platform that spoofs their employers actual platform
- Employee credentials are stolen when employee logs in to fake platform

Payroll Impersonation Fraud

How is it done?

1. The fraudster sends an employee a phishing email that impersonates the human resources or payroll department and the payroll platform
2. The email directs the employee to log in to confirm or update payroll information
3. Employee clicks link or opens attachment in the email and confirms or updates the payroll information
4. The fraudster uses the stolen credential to redirect the payroll to an account controlled by the fraudster

Payroll Impersonation Fraud

Prevention

- Employers
  - Self-service platforms authenticate requests to change payment information using previously known contact information
  - Self-service platforms should reauthenticate users accessing the system from unrecognized devices using previously known contact information
  - Set up alerts on self-service platforms for administrators to flag unusual activity

Payroll Impersonation Fraud

Prevention

- Employees
  - Check the actual sender email address on payroll-related communications
  - Do not enter login credentials when clicking on a link or opening an email
  - Do not reply to suspicious email – check email validity

Resources

- Current Fraud Threats Resource Center
  - https://www.nacha.org/content/current-fraud-threats-resource-center
    - “Protecting Against Fraud” booklet
    - FBI links
    - eResources for online payments

Questions?

Danita Tyrrell, AAP
Director, Network Rules
NACHA
703.561.3937
dtyrrell@nacha.org

NACHA
The Electronic Payments Association®