Business Email Compromise, Vendor Impersonation Fraud, and Payments: What Organizations and Financial Institutions Need to Know

Similar to account takeovers, the roots of this fraudulent activity are not in banking and payment systems themselves, and are not always perpetrated online. Rather, Business Email Compromise and Vendor Impersonation Fraud exploit vulnerabilities and compromises within an organization's own personnel, processes and systems to convince organizations to send payments voluntarily to accounts controlled by the fraudsters.

What Are Business Email Compromise and Vendor Impersonation Fraud?

Business Email Compromise (BEC) and Vendor Impersonation Fraud (VIF), represents risks to businesses, non-profits, and government and other public-sector organizations. With BEC, legitimate business email accounts are either compromised or impersonated, and then used to order or request the transfer of funds. The fraudster will often compromise one of the business's officers and monitor their account for patterns, contacts and information. The fraudster will often wait until the officer is away on business to use the compromised email account to send payment instructions. This makes the payment instructions more difficult to verify, and at the same time, seemingly more legitimate. The payment instructions will direct the funds to an account controlled by the fraudster.

More recently, BEC has targeted real estate buyers and/or sellers. The fraudster represents themselves as lawyers or representative of law firms and claim to be handling confidential or time-sensitive matters related to the sale or closing of real estate.

In other recent cases, BEC schemes have targeted payroll departments or individual employees in attempts to move funds to fraudsters account via an otherwise regular payroll process. If the payroll department is compromised, fraudsters attempt to send fraudulent payroll files, directing funds to accounts they control. If individual employees are compromised, fraudsters often direct the employees to update their payroll information via a fake payroll platform that spoofs an organization's actual payroll platform. The fraudsters then use the stolen employee credentials to change payment information in the real payroll platform. Sometimes fraudsters specifically direct payments to prepaid card accounts.

In instances of VIF, fraudsters impersonate a legitimate vendor or contractor, and contact businesses or public-sector entities requesting to change payment account information. Contact can come in the form of an email, telephone call, fax, or even a letter in the mail. In each case, the fraudster requests that account information payment be changed to account controlled by the fraudster, so that when an invoice is received, the entity processes a payment to the fraudster, resulting in a loss to the entity. Social engineering techniques have grown more sophisticated over time.

Fraudsters may create email addresses that are similar to the actual email address making it difficult to spot. Written correspondence may appear to be printed on legitimate letterhead or stationery.

Although victims of these scams range from small businesses to large corporations, any business entity could be the target of this form of social engineering. In particular, public-

sector entities seem to be targeted because their contracting information is typically a matter of public record. Fraudsters use information from such public records to impersonate legitimate contractors more convincingly.

Sound Business Practices for Businesses and Public-Sector Entities

Every business, nonprofit, government agency or other public-sector entity should evaluate its internal processes and controls to understand its vulnerabilities to these social engineering frauds. Solid internal controls are key to guarding against these scams. Examples of sound business practices include:

- Understand that these types of social engineering attacks are not conducted solely online; the vectors for these attacks can be Internet-based or by phone calls, faxes or letters in the mail.
- Educate and train employees to recognize, question, and independently authenticate changes in payment instructions, requests for secrecy, or pressure to take action quickly.
- Authenticate requests to make payment or change payment information. Use known contact information to authenticate payment or change requests, rather than contact information provided with the change request. For example, use an already known telephone number instead of a number provided in a change request. • Be especially cautious if the request for payment is from a personal email account instead of the company email.
- Review your accounts frequently.
- Initiate payments using dual control — for example, require two people to approve payment initiation or to make changes to payment information, such as recipient information. Not only can this be effective against a single person falling victim to a social engineering fraud, but it can also guard against other types of internal fraud.
- Never provide password, username, authentication credentials, or account information when contacted. Financial institutions will not ask for this information. If in doubt, use a known contact list or publicly available contact information to confirm the validity of the contact.
- Don’t provide other non-public information on social media. Seemingly innocent information can be used to make a fraudster believable when they contact others within the same organization. For example, job duties and descriptions, hierarchal information, and out-of-office details.
- Specifically regarding company email policies:
    - Avoid free web-based email accounts. A company domain should always be used to establish company personnel emails.
    - Consider registering domains that closely resemble the actual company’s domain.
    - Do not use the ‘reply’ option when authenticating emails for payment requests. Instead, use the ‘forward’ option and type in the correct email address or select from a known address book.
- Make vendor payment information forms available only via secure means or to known entities.

- For a self-service payroll platform, require changes to payment account information to be made or confirmed only by site administrators, and use methods like verification codes sent to existing contact information.
- Calls from a financial institution questioning the legitimacy of a payment should be taken seriously.
- Contact your financial institution if you need assistance.

Sound Business Practices for Financial Institutions

NACHA strongly encourages financial institutions to have programs available to help educate and train their clients' employees in sound payments practices and controls. For financial institutions themselves:

- Alert your business customers to these and other types of social engineering scheme.
- Educate business clients and consumers on prevention, detection, and reporting measures.
- Recommend to your originators that they use dual control for payment file initiation.
- Encourage daily review of accounts.