State Bank of India
(California)

Understanding Wire and ACH Fraud

What is Wire Fraud?

Wire transfers are one of the most common methods of money transfer which are used by many businesses because it is an easier way to move money from one bank account to another, anywhere around the world, in a matter of hours.

Wire fraud is any fraudulent activity that occurs over phone lines or involves electronic communication. Most wire fraud occurs when someone other than the authorized accountholder steals or withdraws money from an account online. In many cases seen today, fraud attempts occur through email where criminals use false information and identities to gain access of a bank account. If a payment request is not authenticated, this can result in a fraudulent transfer of money.

Wire fraud typically takes two forms: account takeover and unwitting participation by account holders. Account takeover involves a scammer seizing business or personal information to gain access to the account holder's funds. Unwitting participation occurs when a scammer poses as a government official, relative, an employee, or some other trusted source to trick the accountholder into willingly sending money.

What is an ACH Fraud?

The ACH (Automated Clearing House) network handles millions of electronic financial transfers every day. ACH fraud is theft of funds through the ACH network. This is similar to check fraud and begins with a fraudulent access of online banking credentials. "Payroll" which makes use of ACH network for direct deposits and other transactions is particularly vulnerable to ACH fraud.

How does ACH/Wire fraud occur?

Any cyber fraud can happen over the phone or through web transactions. The most common frauds revolve around email or other types of phishing schemes like:

Malware is a type of malicious software designed to infiltrate and damage computer system without the user's consent. Malware can gain access to a computer when a user opens an email or clicks on a link that redirects to a URL that downloads the malware and infects the computer operating system. Hackers can also send malware through USB flash drives and other forms of removable media. Once inserted, hackers can obtain user credentials to gain access to payment and data systems.

Phishing is the most common type of cyberattack. Phishing occurs when hackers send fraudulent emails that are meant to resemble emails from trusted and reputable sources, like company employees, banks, etc. These emails steal sensitive data like credit card information, log in credentials, and more. Please remember, we will never ask you for your personal information or login credentials via email.

SMS Phishing (Smishing) and Voice Phishing use automated calls or text messages to imitate banks and deceive users into providing personal information by threatening the active status of their accounts. Their personal information is then used to gain access to payment systems or take over accounts. SBIC will never ask you for your personal information or login credentials via text.

Email Account Compromise occurs when cybercriminals use stolen credentials, phishing, or look-alike domains to access an email account. Cybercriminals may impersonate a known employee or vendor to convince another employee to transfer funds to a fraudulent account.

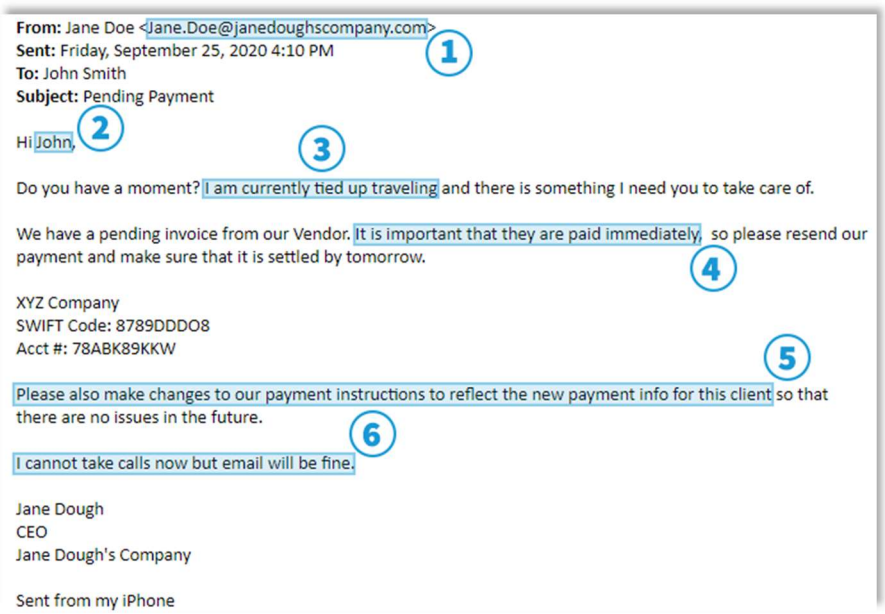
Examples of common scams used by criminals for Wire/ACH fraud

Cyber criminals rely on methods and urgency to trick people into divulging sensitive information or tricking employees into completing fraudulent wire transfers. Here are some common things to look out for that can help in identifying fraudulent emails:

INTERNAL EMPLOYEE/EXECUTIVE SPOOFING

Cyber criminals can target victims by impersonating a fellow employee or known executive at the victim's company.

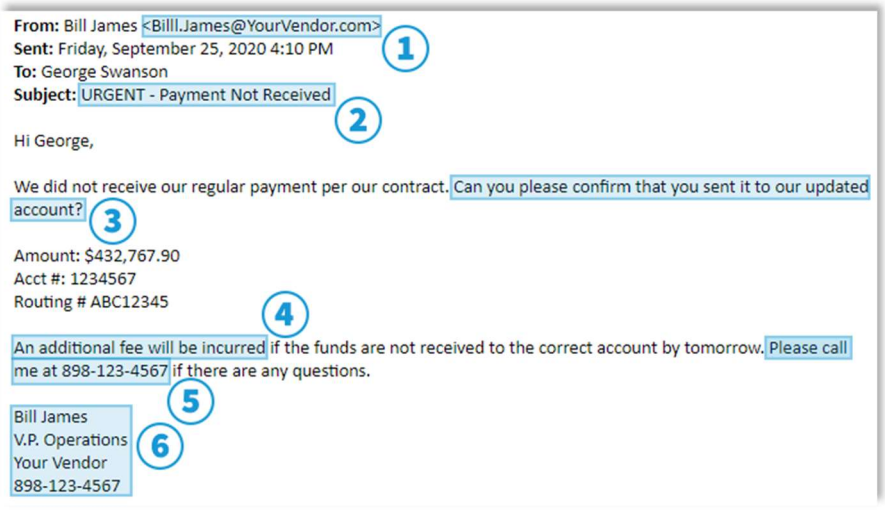
1. Spoofed email address. Look for return addresses that you don't recognize, have inconsistent or incorrect spelling, or don't match the sender name. In this case, the sender's last name "Doe" does not match the spelling of "dough" in the domain name.
2. Familiar greeting
3. Look out for emails where the sender mentions they are away or out of the country.
4. Urgent requests to resend are highly suspicious.
5. Requests to modify payment instructions, including the receiving account listed, should follow your company's internal procedures. This includes confirming requests with a known contact using a phone number on file.
6. If the sender claims to be unavailable via phone and can only take emails, this should be a red flag.



VENDOR SPOOFING

Cyber criminals can also target company employees by impersonating a client or known vendor.

1. In this case, the return address appears to be from a known vendor, but the first name in the return address is spelled incorrectly.
2. Urgency in the request
3. Always look out for a sender looking to modify payment details or information via email.
4. Sender does not have the authority to amend a contract or impose additional fees via written or verbal communication.
5. Always defer to contact information listed on file as opposed to sent via email.
6. Fake email signature



Fraud can be prevented from occurring within your company, but you must be proactive about cybersecurity.

Here are some best practices to help prevent online fraud:

- Make sure to have a company policy and procedure regarding wire transfers and other banking activity, and that all the employees within the company understand and practice the same.
- Be wary of suspicious email-only wire transfer requests and requests involving urgency.
- Always verify the authenticity of each transaction such as an ACH or a wire transfer request within your company by calling the authorizer on their direct line, and NOT just by replying to the email or calling the phone number listed in the email.
    - Always follow this practice even if the email is received from a known party/vendor.
- Make use of call-back verification process when setting up payment instructions for a new vendor or making changes to payment instructions of an existing vendor.
- It is a best practice to use a second individual to verify the transaction within your business for authorization of all online transfer or payment requests.
- Monitor your company's bank accounts daily.
- Never share username and password information for online services with third-party providers or to other individuals.
- Avoid using an automatic login feature, that saves username and password for online banking.
- Never access bank, brokerage or other financial services information at internet cafes, public libraries, etc. Unauthorized software may have been installed to trap your account number and sign-on information leaving you vulnerable to possible fraud.
- Ensure your device has virus protection and security software which are updated regularly.

What should you do if you think you have been a victim of fraud?

1. Act quickly. Immediately escalate any suspicious transactions to your bank, particularly ACH or wire transfers. These types of transactions occur quickly and difficult to recover. However, immediate escalation may help in preventing further losses.
2. Contact the wire service that transmitted the funds. They will have records showing where the funds were sent. If reported quickly, they may be able to freeze the funds and open their own investigation.
3. Contact the FBI. The FBI is usually the authority to investigate wire fraud. Go to the FBI's Report Threats and Crime page to submit a report.
4. Reach out to your company's IT team. They should scan your organization's computer network for any signs of malware or other affected systems.

BE ALERT!
Knowing how a scammer works and being aware of the resources available
can help you protect yourself and avoid cyber fraud.