Fraud Awareness:

Best Practices & Red Flags

Corpay is a major participant when utilizing the financial system to effect and promote the business interests of our customers. As such, we understand and take our role in ensuring that we and our customers can confidently operate efficiently and securely seriously.

We would like to remind our customers, our valued Financial Institution partners, and any other company with downstream beneficiaires and vendors, to be extra diligent during this time of uncertainty. Increasingly, instances of fraud are becoming more common, with many arising from the current situation.

As the economic situation resulting from the COVID-19 continues to unfold, many companies and institutions have activated their Business Continuity Plans, including special accommodations such as working from home or interim changes in established protocols.

With instances of fraud are becoming more common across the country, at Corpay we have also seen a material uptick in fraudulent cross border transactions experienced by both companies and consumers. Based on investigation metrics, our findings indicate that approximately 80% of cases are due to social engineering and business email phishing and/or compromise of either the remitter or beneficiary. Fraud schemes are becoming increasingly sophisticated, often with an impersonator monitoring communication and email activity over a period of time, waiting for an opportunity to exploit a situation. Often, this results in fraudulent payment instructions being inadvertently sent.

Read on to learn about the best practices you can use to detect and mitigate fraud. These practices include red flags to keep an eye out for, and some basic recommentations for yourself and your company to follow.

Best Practices

- Consumer/Commercial clients should verify details of all orders, before submitting a payment for processing. For new or potential unusual transactions (that don't align with historical payments), verbal confirmation by phone is recommended.
- Check email addresses carefully. Often the fraudster will make a subtle change to the email address (for example, changing a "o" to "0" or omitting a letter) and impersonate the user – and later intervene communications.
- See more information on identifying a phishing mail in the security guidelines for online activity section on our website.
- Confirm that you have the correct authorized individuals, with current contact details documented that can place an order for a cross border payment.
- Follow internal policies and procedures each and every time.

Red Flags

- A request to change the account number or banking details of an existing beneficiary.
- Unusual cross border payment activity: an international payment is requested that does not fall into your beneficiary/vendor's normal activity. Did your beneficiary/vendor verbally confirm this invoice internally?
- Unusual wire or series of payments to China, Hong Kong or Africa: is this the first time? What is the specific purpose? Is there a matching invoice? Does it look legitimate? Be vigilant with your questioning and escalate if it seems suspicious.
- Key contacts are unavailable: it is not unusual for a fraudster to have access to calendars and to wait for an opportunity to strike when key contacts are not easily reached.
- Email for a transaction request is received outside of regular working hours.

It is critically important to remember that a domestic payment falls under the juristiction in which it's being received. An international payment, once released, could touch multiple international jurisdictions, and so successful retrieval of funds is limited. One main reason is the fraudster has a plan to immediately withdraw the proceeds, or transfer funds to another account. Laws and their enforcement can and do vary from country to country.

Have you been compromised?

- Contact Corpay urgently. Time is of the essence; while recall success is never guaranteed, a recall's success chances improve if both of these are true: 1) fraud can be verified, and 2) funds are still on account at the receiving bank.
- Provide clear and complete information to Corpau; fraud transactions trigger special protocol by all parties involved in the transfer funds.
- Contact local authorities.
- Depending on the value of the payment, you may wish to hire legal counsel in the destination country.

Fraud Awareness: Social Engineering

Corpay is a major participant when utilizing the financial system to effect and promote the business interests of our customers. As such, we understand and take our role in ensuring that we and our customers can confidently operate efficiently and securely seriously.

It is possible to detect and prevent fraud. Regardless of how secure your business is, it is often the human element that falls prey to social engineering methods. While you cannot discount the human element, you can learn to anticipate how employees and colleagues might fall victim to social engineering tactics and develop measures to mitigate the risk.

Nefarious characters will go to great lengths to educate themselves on the inner workings of your business, your activities, your processes, and employees. **Wire and Email Fraud** are highly successful and lucrative for fraudsters and are relatively easy to pull off with a little research and clever tactics. The first step in risk mitigation is to understand the most common types of social engineering scams that have befallen many businesses.

Some common social engineering tactics are **Caller ID and Email Spoofing**. It is relatively simple to make an email or caller ID appear to be legitimate or seemingly match one that you/your employees are used to seeing on a regular basis. That email from your vendor asking you to update the bank account information appears completely legitimate - doesn't it? Or that email from your company President asking you to send funds to him while travelling?

If it was fraudulent, your firewalls and security features would catch it - right? You could be very Wrong!

Unfortunately for several businesses by the time a scam has been detected, it is far too late.

Pretexting

Criminals create a false 'pretext' for contacting one of your employees. They may pretend they are a prospective supplier, research firm, bank or government agency asking for the names of employees, banking information, login credentials or something seeming equally as innocuous. Any information they gain can thereafter be used to build a profile which in turn allows the fraudster to pose as an employee and ultimately gain access to your business, personal or financial information, your systems or customers. They may move on to scam your business using **Caller ID or Email Spoofing**.

Phishing

[pronounced Fishing] is a very common online scam. An email is sent with the intent to manipulate the recipient into disclosing personal, business or financial information. Typically, these phishing scams attempt to play on emotions or sympathies. They will stress an urgency and will contain a link often accompanied by a deadline date for you to access and input your information. By disclosing any of these details you are essentially putting the fraudster a step closer to accessing your accounts. Fraud can have far reaching and devastating impact to your life or business. **A legitimate urgent situation would never require anyone to send personal, business or financial information by accessing a link.**

Characteristics and Behaviors to always be aware of

- Text contains incorrect spelling, phrasing or grammar or uses wording that is uncharacteristic
- Customer is difficult to contact and prefers email communication
- Email address differs very slightly from that which you are used to
- Email domain is different from that which you have historically used or is from a free
- service provider such as Hotmail or Gmail when it should contain a business domain
- Transaction may be inconsistent with historical transactions
- Contact applies significant pressure for the deal to be processed prior to receiving full verification
- Unexplained sense of urgency and a willingness to accept shortcuts
- Unexpected changes to payment or beneficiary details

How do you protect your business?

We recommend taking steps similar to what Corpay does. Awareness and Training are key. Employ tactics that are designed to verify and validate the information your employee is receiving, before making any changes to payment details.

If you receive an email request to alter banking information, phone your contact at your vendor's company to verify that banking information has been changed.

If you receive a phone call requesting a change to banking information, take the time to place a phone call to the number you have always used for your contact – not the phone number that just appeared on caller ID when the request to change banking information was received – and verify that banking or payment details have changed. You may just learn that your or your vendor's email or phone network have been compromised, and by taking the few minutes to verify the information you have just saved you and your vendor from being scammed.

Corpay

Corpay.com