ConnectPay

The Fraud Memo

ConnectPay

Fraud and scams are just the latest challenge for organizations, businesses, and individual clients. There is no company in the world that has immunity from fraud. Companies should still expect criminal activity and fraud incidents to grow. **ConnectPay** wishes to inform you of the most popular fraud scenarios and to assist in this fight.

What is the damage caused by fraud?

Fraud losses are complex. Some costs can be tallied: direct financial loss or costs due to fines, penalties, responses, and remediation. But some costs are not easily quantified — including brand damage, loss of market position, employee morale, and lost future opportunities.

What are the most common forms of fraud?

- **Occupational fraud** is when an employee, management, officer, or owner of a company commits fraud against the company. Corruption, Asset Misappropriation, and False Statements are the three main categories of occupational fraud. According to the ACFE, this type of fraud causes the company to lose the most money, up to 5% of its total revenue.

- **Identity Theft** – This type of attack occurs when someone obtains the victim's personal information and uses it without permission to commit fraud.

- **Friendly fraud** – similar to identity fraud, except the perpetrator is from the victim's close environment. As a result, the fraudster obtains the victim's personal information and utilizes it to commit fraud without their authorization. It might be a family member, close friend, roommate, colleague and etc.

- **Account takeovers** - a type of identity theft and fraud in which a malicious third party gains access to a user's account credentials.

- **Hacking** – The two most common types of hacking are email and system hacking. These incidents occur when cybercriminals gain unauthorized access to your emails or systems and are able to view and/or manipulate the information contained within them.

- **Phishing** – a very common form of cybertheft. These attacks occur when cybercriminals steal private data from a victim by using a fake website that looks to be authentic. The majority of the time, unknowingly, individuals are introduced to these websites in the form of email.

ConnectPay

- **Social Engineering** – With social engineering, attackers can build trust with an individual through social interactions in order to gather information about the person, system, or organization in question.
- **CEO fraud**, also known as Business Email Compromise (BEC) – is a type of fraud that is enabled via social engineering. Fraudsters pose as a high-ranking executive (usually the CEO) in order to persuade employees to make a payment, provide confidential information, and so forth.

- **Malware Threats** – Hackers can send malware to your devices or online platforms in order to gain access to your personal information by using malicious software (also known as malicious software). Even if it does not affect the physical hardware of your systems or equipment, data and software within them can be severely damaged.

What kind of preventative measures should be taken?

- Implement proper fraud detection, response, and prevention strategy within your organization. To prevent fraud and misconduct from occurring in the first place, to detect fraud and misconduct when it does occur, and to take appropriate response actions. There should be defined duties and responsibilities for employees, along with a zero-tolerance fraud culture. The presence of Anti-Fraud Controls is associated with lower fraud losses and quicker detection.

- Create Fraud awareness within your company. Be sure to educate your employees on fraud prevention best practices and warning signs, as well as procedures to follow in the event of an attack.

- Turn on two-factor authentication wherever possible, and don't disclose one-time passcodes by text or phone call. Consider using strong passwords or a password manager if your site does not support two-factor authentication.

- Never give out your login credentials, PIN, password, one-time passcode, or personal information over the phone or to live chat support. Your login information must be secure and kept confidential. Do not use the same passcodes and passwords for different applications. Sharing this kind of information is tantamount to sharing full access to your funds.

- Secure your devices – Users should protect their internet and mobile devices by encrypting data stored on them, staying away from public Wi-Fi, utilizing a VPN, and installing anti-malware. All devices should have anti-malware protection.

ConnectPay

Important Information

For more information on how to stay secure and prevent fraud, click here https://connectpay.com/security/

Please always inform **ConnectPay** about suspicious activities: fraud@connectpay.com.