ConnectPay

The Fraud Memo

ConnectPay

At a time when the entire world is fighting a global pandemic, organizations and businesses face a different major foe that is becoming more aggressive: fraud. There is no company in the world which has an immunity from fraud, there is no vaccine either to protect from fraud. In 2022 companies should still expect criminal activity and fraud incidents to grow. **ConnectPay** wishes to inform you of the most recent fraud trends and to assist in this fight.

1. What are the current fraud trends?

According to the research of the Association of Certified Fraud Examiners (ACFE), **51%** of organizations have discovered more fraud since the beginning of the pandemic, and **71%** of enterprises and organizations estimate the amount of fraud in their organizations to rise by 2022.

For the year 2021, **38%** of organizations have decided to increase their investment for anti-fraud technologies. In response to the pandemic, **80%** of the organizations surveyed have already made one or more adjustments to their anti-fraud programs.

There was a nearly equal split between frauds committed by internal and external perpetrators, at nearly **40%** each – with the remainder largely due to collusion between the two. Business partners remain a risk and fraud committed by management is trending upward.

According to PwC's Global Economic Crime and Fraud Survey 2020 nearly half of organisations had suffered at least one fraud incident – with an average of six fraud incidents per company. The most common types were:

- customer fraud
- cybercrime
- asset misappropriation
- bribery and corruption
- accounting/financial statement fraud

2. 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.

The average financial loss might range between 0.5 and 5 percent of total typical organization revenue. According to Javelin's 2021 Identity Fraud Study, identity fraud losses in 2020 amounted to 56 billion USD. According to the 2020 ACFE Report to the Nations, a typical occupational fraud case lasts 14 months before detection and causes a monthly loss of 8 300 USD. The importance of timing in this case cannot be overstated; the later the fraud is discovered, the greater the loss.

3. 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 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 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 cyber criminals gain unauthorized access to your emails or systems and are able to view and/or manipulate the information contained within them.

- **Phishing** – 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.

- **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.

ConnectPay

4. What kind of preventative measures should be taken?

- Implement proper fraud detection, response, and prevention strategy within your organisation. 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. 33% of occupational fraud cases were discovered because the whistleblower process was implemented and employees were familiar with it, according to the ACFE.

- 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.

- 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.

5. 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: support@connectpay.com.

Sources of Information

Javelin: https://www.javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study
the Association of Certified Fraud Examiners – ACFE: https://www.acfe.com/covidreport.aspx & 2020 ACFE Report to the Nations
PwC: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
UK Finance: https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
Murray Goldstein: https://www.coxblue.com/4-ways-small-businesses-can-protect-themselves-from-cyber-attacks/