Cyber Fraud in Vietnam: Law and Practice

By Duc Anh Tran and Chi Phuong Nguyen

Recently, Vietnam has witnessed a dramatic increase in cyber fraud, causing significant financial losses and posing a grave threat to both Vietnamese and foreign entities. With the increasing reliance on digital technology and the widespread adoption of online platforms, the country has become fertile ground for cybercriminals to exploit vulnerabilities and conduct various fraudulent activities. This article aims to present an overview of addressing cyber fraud in Vietnam and offers practical advice for businesses to safeguard themselves from becoming victims of such illicit activities.

Current Situation of Cyber Fraud in Vietnam

In 2023, a report by the Global Anti-Scam Alliance (GASA) identified Vietnam as the developing country losing the second highest percentage of its GDP to scams, with a total loss of VND 91.8 trillion (USD 16.23 billion), equivalent to 3.6% of the nation's GDP.

According to records from the Department of Information Security under the Ministry of Information and Communications, in the first 6 months of 2023, the situation of online fraud in Vietnam increased by 65% over the same period last year; and by 38% compared to the last 6 months of 2022.

Over time, cyber fraud in Vietnam has gradually become more sophisticated and professional. The number of victims and the value of damages caused by this fraud in Vietnam have also increased dramatically. It is worth noting that victims of such crimes are not only individuals and businesses within the country but also foreign entities engaged in business relations in Vietnam. There are even cases where foreign businesses, despite having no operation or relationship in Vietnam, have been deceived into transferring funds to accounts opened within the country.

The increase in cyber fraud in Vietnam can be attributed to many causes, but some typical factors can be listed as follows.

- Vietnam's growing economy has attracted foreign investment and businesses, making it an enticing target for cybercriminals who seek financial gains. The valuable data and financial transactions associated with this economic growth serve as motivation for cybercriminals to target individuals, organizations, and even government entities.
- Vietnam's ongoing digital transformation initiatives, which promote internet banking and online transactions for convenience, have inadvertently created opportunities for cybercriminals to exploit the system to easily open fraudulent bank accounts and misappropriate funds.
- International cybercriminals tend to transfer money to developing countries like Vietnam, where there might be less-stringent regulations, more limited infrastructure, and less experience in handling fraud, to more easily withdraw and handle the ill-gotten money.

Common Types of Cyber Fraud for Businesses

Both domestic and foreign businesses in Vietnam are becoming preferred victims of cyber criminals due to the large size and value of their transactions compared to individuals. Many tricks and techniques are skillfully used to lure an entity into a trap, including:

- **Phishing:** Fraudsters employ tactics of sending misleading emails or establishing fake websites that appear authentic and legitimate, then tricking employees into revealing sensitive information such as login credentials, financial details, or customer data.
- **Business Email Compromise (BEC):** Fraudsters impersonate company executives or vendors and send fraudulent emails requesting payments or sensitive information. In some instances, the fraudsters set up email accounts that resemble those of business partners of targeted companies. They will then steal the information of transactions between parties and send emails requesting the companies to transfer money for business contracts to the fraudster's accounts.
- **Vendor or Supplier Fraud:** Fraudulent vendors or suppliers may deceive businesses by providing substandard products or services, overcharging, or not delivering as promised. Once they receive the deposit/payment for goods into their bank accounts, they will immediately cut off communication and disappear. This type of fraud can result in great financial loss and harm to the company's reputation.
- **Ransomware Attacks:** Cyber criminals infect a company's network with malicious software that encrypts data and demands a ransom for its release. Failure to comply with the ransom demands can result in permanent loss or exposure of the data.

Current Regulatory Framework Sanctioning Cyber Fraud in Vietnam

The main legislation sanctioning cyber fraud in Vietnam is the 2015 Criminal Code, as amended in 2017 ("Criminal Code") and Decree No. 144/2021/ND-CP on administrative penalties for violations against regulations on social security, order, and safety; combating social evils; firefighting and prevention; rescue; and prevention and control of domestic violence ("Decree 144").

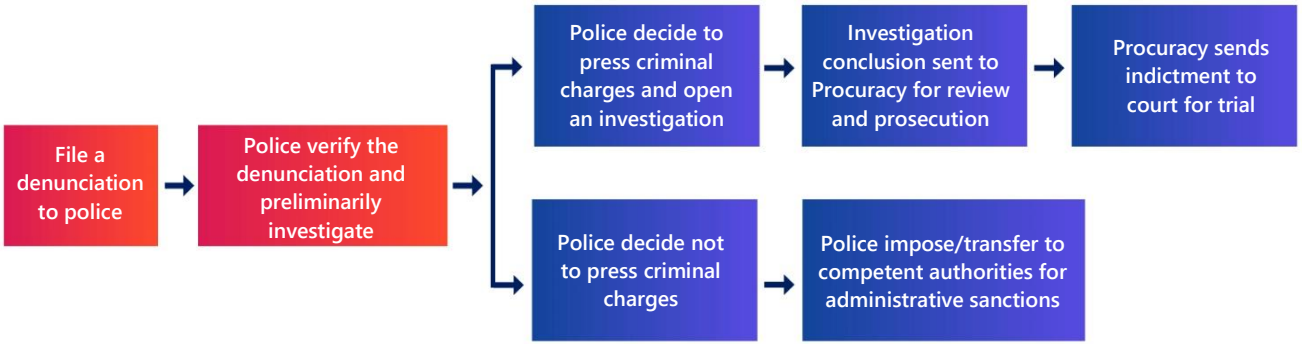
The Criminal Code has a specific section (Section 2 of Chapter XXI) stipulating crimes against regulations on information technology and telecom networks. Accordingly, depending on the nature of the acts, cyber fraud might fall within the scope of Article 290 (Crime of using computer networks, telecom networks, or electronic means to commit acts of property appropriation) or Article 174 (Obtaining property by fraud). The sanctions can include a noncustodial reform sentence or imprisonment; monetary fines; prohibition from holding certain positions, practicing certain professions, or doing certain jobs; or partial or complete confiscation of assets.

If the infringing act is not sufficient to constitute a crime under the Criminal Code, it might be subject to administrative sanctions specified under Article 15 of Decree 144. These sanctions could include a relatively small monetary fine and confiscation of exhibits and means used for committing the administrative violation, such as the violator's computer or phone.

Based on our experience and observations, cyber fraud, especially in cross-border cases, is frequently characterized by high levels of sophistication and professional organization. These activities often operate on a large network scale, with the primary objective of misappropriating substantial amounts of money. This type of cyber fraud in Vietnam generally constitutes a criminal offense under the Criminal Code, rather than being subject to administrative sanctions.

Procedures for Handling Cyber Fraud in Vietnam

The Vietnamese enforcement agencies in charge of addressing cyber fraud cases, notably the Criminal Police Department (C02) working in collaboration with the Department of Cybersecurity and High-Tech Crime Prevention and Control (A05), have demonstrated their effectiveness and considerable expertise. Handling cyber fraud in Vietnam normally involves the following main stages:



The duration for resolving a cyber fraud case varies depending on its severity and complexity. For a typical criminal case, it can take approximately 5 to 22 months from the receipt of the denunciation to the issuance of the first-instance judgment. However, cyber fraud cases often require more time due to their complicated nature. These cases involve highly sophisticated techniques, necessitating expertise in both investigative and IT skills to track down the fraudsters. In cases of cross-border fraud, which involve foreign entities, the process of gathering sufficient evidence in the investigation will be prolonged, because most of the evidence collection will be sent through diplomatic channels and require close coordination between Vietnamese law enforcement and the foreign authorities and entities being asked for evidence or testimony.

Challenges in Handling Cyber Fraud

The biggest challenge in handling cyber fraud is tracing cyber criminals. High-tech criminals, such as cyber fraudsters, usually have accomplices and are professionally organized. Some criminal organizations operate across borders and include individuals of different nationalities. The cross-border nature of cyber fraud makes it difficult for law enforcement agencies to coordinate efforts and bring the culprits to justice. Moreover, the criminals often employ sophisticated techniques to conceal their real identities and locations, making it difficult to track them down.

The integrity of electronic data, which is crucial for proving crimes, is highly vulnerable to alteration or deletion in cyber fraud cases. Gathering electronic evidence becomes an arduous task in many cases, as criminals, upon realizing that their illegal activities are at risk of exposure, frequently resort to crashing websites or deleting relevant information, leading to irretrievable evidence.

The process of collecting data in cyber fraud cases often requires collaboration from service providers, typically website/domain developers or banks, both domestic and international. However, these service providers frequently employ customer confidentiality as a justification to deny or delay the provision of requested information, making it even more challenging to collect necessary evidence.

These factors prolong the investigation of enforcement agencies, causing the victim to experience constant anxiety and irreparable damages. Even in cases where the fraudsters are successfully tracked down, it does not guarantee the full reimbursement of appropriated money.

Recommendations for Risk Prevention

To reduce the risk of falling victim to cyber fraud, businesses should heed the following recommendations:

1	It is important to develop a comprehensive cybersecurity system and policy for your organization. This involves implementing robust firewalls, intrusion detection systems, and antivirus software to protect the internal network from external threats. Additionally, businesses should establish a cybersecurity policy that outlines guidelines, procedures, and responsibilities for employees regarding data protection, access controls, and incident response.
2	Ensure that all staff are careful with suspicious emails, messages, or calls that request business information or financial details. Avoid clicking on links or downloading attachments from unknown or untrusted sources. Verify the legitimacy of any communication by independently contacting your business partners through any other official channels, rather than just email.
3	Never transfer money to an unfamiliar bank account without clearly double-checking the written request. Even if the requester is your long-term and trusted partner, do not be rule out the possibility of someone faking/hacking into your partner's email to make a request.
4	If you become a victim of cyber fraud, report the case immediately upon discovery to your financial institutions and local authorities. Timing is the most important factor in cyber fraud cases, because if the detection and response is timely, banks and local authorities can hold the payment or freeze the fraudulent bank accounts to prevent fraudsters from dispersing the money. In the meantime, you should collect and preserve evidence showing the fraud and submit it along with the denunciation to the police.
5	If you fall victim to cyber fraud in Vietnam, consult a local attorney. Local attorneys possess a deep understanding of the legal system and have extensive experience working with local banks and the police, which facilitates tracking down fraudsters. By consulting a local attorney, you can benefit from their specialized knowledge and guidance to navigate the case and increase the chances of recovering your losses.

Contact Us

If you have been a victim of cyber fraud in Vietnam, or require further information about the topic, please contact us at vietnam@tilleke.com. Our lawyers are well-placed to assist clients effectively and efficiently, with extensive experience and knowledge not only about statutory procedures but also practical norms in Vietnam. Through our close collaboration with local associate firm T&G Law Firm LLC (TGVN), we are also able to advise clients on case strategy for disputes and provide representation before Vietnamese courts and other authorities.