DORSEY
DORSEY + WHITNEY LLP

Recent Trends in Wire Fraud Scams: Uncovering and Tackling the Latest Tactics in Hong Kong

by Janet Wong and Steven C. Nelson

Wire fraud threats have been on the rise in recent years, with Hong Kong becoming a particularly attractive destination for fraudsters due to its status as a global financial hub. Criminals are using increasingly sophisticated tactics, including fake email addresses and websites, to carry out email wire fraud scams and trick individuals and businesses into wiring funds to unauthorized recipients.

According to the Hong Kong Police Force (HKPF) press conference held on February 14, 2023, there was a significant increase of 45.1% in deception cases in 2022, with the total number rising to 27,923. Over 70% of these cases were internet-related. The primary drivers behind this increase were online shopping scams (8,735 cases), employment fraud (2,996 cases), investment fraud (2,850 cases), and telephone deception (2,831 cases), with increases ranging from 40% to 1.8 folds. The large amounts involved in investment fraud and telephone deception, which exceeded HK$1.8 billion and HK$1 billion respectively, remained a cause for concern.[1]

Newer Types of Wire Fraud Scams

As the digital landscape continues to evolve, fraudsters are not only adapting their tactics but also devising new methods of exploitation. While traditional types of fraud, such as CEO scams and Business Email Compromise (BEC) scams, persist, criminals are increasingly focusing on emerging technologies and trends to perpetrate innovative forms of wire fraud. By staying aware of these evolving threats, individuals and businesses can better protect themselves from falling victim to these sophisticated schemes. Some of the newer types of scams include:

1. **Cryptocurrency and NFT investment scams**: Taking advantage of the rising popularity of digital assets like cryptocurrencies and non-fungible tokens (NFTs), scammers are enticing victims with false promises of high returns on investments. They employ tactics such as creating fake websites, social media accounts, and online investment platforms to make their schemes appear legitimate.
2. **Personal data fraud**: This type of fraud encompasses a wide range of illicit activities

Related People

- Janet Wong
- Steven C. Nelson

Related Capabilities

- Financial Services Regulatory
- Privacy & Social Media
- Asia-Pacific
- China

involving stolen personal data, including fraudulent bank transfers, identity theft or impersonation, and phishing scams where individuals are tricked into providing personal data to fraudulent websites or emails. Scammers may also use unlawfully obtained personal data to commit financial or other types of crime.

3. **Online shopping scams**: With the rise of e-commerce, online shopping scams are becoming increasingly common. Fraudsters typically create fake websites or online marketplaces, offering high-demand or luxury items at significantly discounted prices. Once the victim makes a payment, the scammers either fail to deliver the promised goods or send counterfeit or inferior products.
4. **COVID-19 related scams**: The ongoing pandemic has given rise to a new wave of scams, such as fake vaccination appointments, bogus online sales of personal protective equipment (PPE), and fraudulent COVID-19 testing services. Scammers exploit the public's fear and uncertainty surrounding the pandemic to defraud unsuspecting victims.

Hong Kong Wire Fraud Updates

Hong Kong has taken several measures to combat wire fraud scams in recent years:

1. **Establishment of the Anti-Deception Coordination Centre (ADCC)**: Established in 2017, the ADCC is a cross-departmental unit that coordinates efforts to combat wire fraud in Hong Kong. The ADCC works closely with law enforcement agencies, financial institutions, and other organizations to raise awareness of fraud risks and to improve the detection and prevention of fraudulent activities. In 2022, the ADCC has significantly contributed to the fight against wire fraud scams by intercepting over HK$1.3 billion of payments, preventing victims in over 500 deception cases from wiring money to fraudsters. Additionally, the HKPF had intensified intelligence-led operations, leading to the neutralization of multiple deception syndicates and the arrest of about 1,300 individuals involved in such activities. As part of these efforts, the HKPF successfully carried out Operation UPSHORE, which resulted in the detection of 410 telephone deception cases, the arrest of 205 persons, and the interception of over HK$20 million of involved assets.[2] The ADCC's continuous efforts and collaboration with other agencies have significantly contributed to the reduction of wire fraud scams in Hong Kong.
2. **Letter of No Consent issued by HKPF**: Under the "No Consent Regime," the HKPF can issue a Letter of No Consent (LNC) to banks to informally freeze bank accounts with suspected fraudulent transfers before formal restraint orders on those bank accounts are applied for and obtained from the Court. The minimum threshold for the HKPF to issue an LNC in cases of suspected fraudulent transfer is HK$100,000 (approximately US$12,820). In late 2021, Hong Kong Court of First Instance issued its judgment in *Tam Sze Leung & Ors. v. Commissioner of Police* [2021] HKCFI 3118, which found the longstanding practice of using LNCs to be unlawful for being *ultra vires* the Organized & Serious Crime Ordinance (Cap. 455, *Laws of Hong Kong*), not being prescribed by law, and being a disproportionate interference with the fundamental right to use property under Article 105 of the Basic Law.

   On April 14, 2023, the Hong Kong Court of Appeal reversed the Court of First Instance decision and upheld the constitutionality of the "No Consent Regime" in its judgment in *Tam Sze Leung & Ors. v. Commissioner of Police* [2023] HKCA 537. This appeal decision is undoubtedly good news for the victims of cyber fraud, who often require an early issuance of an LNC to preserve potential proceeds of crime within a race against time.

Nevertheless, it is important to note that the HKPF only issue LNCs to freeze bank accounts temporarily and the LNCs are usually reviewed regularly and should normally not last for too long. On the other hand, banks are required to act in accordance with its own assessment and generally do not freeze a bank account for very long against a customer's wishes without a court order. To be safe, the HKPF generally recommend that a victim bring urgent civil proceedings in Hong Kong Courts against the persons holding or having an interest in the funds sought to be recovered, for example, by seeking an urgent *ex-parte* injunction order to freeze the bank account to ensure that the funds can no longer be accessed by the fraudsters.

3. **Personal Data (Privacy) Commissioner (PDPC)**: The PDPC has taken various initiatives to protect personal data, including organizing webinars to educate the public and organizations about their rights and responsibilities under the Personal Data (Privacy) Ordinance (Cap. 486, *Laws of Hong Kong*).The PDPC also works closely with other regulatory bodies and law enforcement agencies to combat personal data fraud and other forms of cybercrime. They collaborate on investigations and share intelligence to identify and prosecute those who engage in illegal activities related to personal data.
4. **Launch of "Scameter+" mobile app**: In February 2023, the HKPF introduced the "Scameter+" mobile app as an extension of the Scameter search engine to help the public identify potential frauds and online pitfalls. The app allows users to quickly assess the risk of fraud by entering platform account names or numbers, payment accounts, phone numbers, email addresses, or URLs. Scameter+ also provides scam prevention advice, real-time push notifications, and enables users to view and share anti-scam information. The data in the Scameter series come from various sources, including public reports to the HKPF, information provided by organizations, suspicious phone number databases, and real-time analysis from information security companies. By making this tool easily accessible on mobile devices, the HKPF aims to increase public awareness and empower individuals to protect themselves against potential wire fraud scams. Please visit the Scameter website to download the "Scameter+" App:https://cyberdefender.hk/en-us/scameter/.

Practical Tips and Key Takeaways

The rising trend of wire fraud in Hong Kong and the increasingly sophisticated tactics employed by fraudsters underline the importance of staying vigilant and well-informed about fraud prevention. Individuals and businesses should be aware of the different types of fraud and take necessary precautions to protect themselves against scams.

Here are some practical tips and takeaways for individuals and businesses:

1. ***Be proactive in fraud prevention***: Implement robust security measures, such as two-factor authentication and employee training, to minimize the risk of falling victim to wire fraud scams. Stay informed about the latest fraud tactics and trends.
2. ***Act quickly***: If you suspect wire fraud, immediately contact your bank to report the incident and request a hold on the transaction or a recall of the funds. **Time is of the essence** in these situations, as acting quickly can significantly increase your chances of recovering your funds.
3. ***Contact a lawyer***: Engage a trusted lawyer or solicitor with experience in fraud recovery cases as soon as possible. They can help you navigate the complex legal landscape, file a report with the HKPF, and initiate civil proceedings to recover your funds.
4. ***Understand your legal options***: A knowledgeable wire fraud lawyer can guide you

through the available legal avenues for tracing and recovering your funds. These may include applying for injunction orders, disclosure orders, or utilizing discovery tools such as the *Norwich Pharmacal* application and applications under Section 21 of the Evidence Ordinance (Cap. 8, *Laws of Hong Kong*).

5. ***Collaborate with law enforcement***: Cooperate with the HKPF and other relevant agencies to share information and assist in their investigations. This collaboration can help to identify and prosecute the fraudsters, ultimately contributing to the fight against wire fraud.
6. ***Purchase cybercrime insurance***: Cybercrime insurance can provide coverage for financial losses resulting from wire fraud, data breaches, and other cyber-related incidents. It may cover expenses such as legal fees, investigation costs, public relations efforts, notification expenses, and regulatory fines. Ensure that you work with a knowledgeable insurance agent or broker to customize your policy to meet your specific needs and guarantee adequate coverage against various cyber risks.
7. ***Stay vigilant***: Even after recovering your funds, it is essential to maintain vigilance and continuously update your security measures to safeguard against future threats. Regularly review your internal processes and procedures, and train your employees on how to recognize and respond to possible fraud attempts.

By staying informed and proactive in the fight against wire fraud, individuals and businesses can better protect their assets and contribute to a safer and more secure financial environment in Hong Kong. In light of the potential threats, it is advisable to seek legal guidance from a lawyer experienced in dealing with wire fraud cases. Our wire fraud lawyers in Hong Kong are ready to assist you in navigating these complex issues and providing expert advice tailored to your specific needs.

To learn more about email wire fraud and business email scams, we recommend reading our in-depth guide on protecting against such scams and recovering funds wired to Hong Kong. Our experienced Hong Kong and U.S. wire fraud lawyers have handled numerous cross-border wire fraud cases and are well-equipped to provide expert assistance and guidance. Please visit our **International Cyber Crime and Asset Recovery** page.

Our specific articles include:

- **Guide to Protecting Against Business Compromise Scams, and Recovering Funds Wired to the United States**
- **Guide to Protecting Against Email Wire Fraud Scams and Recovering Funds Wired to Hong Kong**
- **Hong Kong Email Wire Fraud Epidemic**
- **Hong Kong and Overseas Businesses Defrauded of over HK$1.8 billion (US$231m) in 2016**

Contact one of our wire fraud lawyers for further assistance and guidance in tackling cross-border wire fraud cases.

Janet Wong, Partner

Steve Nelson, Senior Partner

Joshua Colangelo-Bryan, Of Counsel

[1]See https://www.police.gov.hk/ppp_en/01_about_us/cp_ye.html

[2]See https://www.info.gov.hk/gia/general/202302/14/P2023021400644.htm