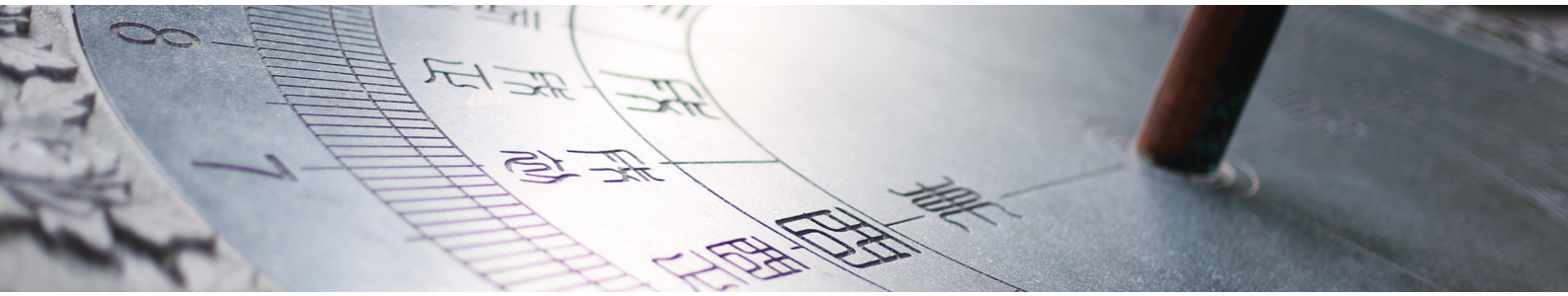
GALL

Eugene Thuraisingam LLP



WIRE FRAUD AND RECOVERY OPTIONS IN HONG KONG AND SINGAPORE

Recent Trends in Types of Wire Fraud

There has been a dramatic increase in wire fraud globally. Hong Kong and Singapore are no exceptions.

According to the Cyber Security and Technology Crime Bureau of the Hong Kong Police Force, in 2021, there were approximately 16,159 reported cases of technology crime, of which there were at least 1,659 romance scam cases, 980 online investment frauds, and 549 email scam cases, which are the most common types of scams we encounter in our practice. The remaining reported cases included credit card fraud and social media scams.

The Singapore Police Force ("**SPF**") in its Annual Crime Brief 2021 similarly reported an uptick in technology-related fraud cases. There were at least 1,099 romance scams, 2,476 investment scams, and 2,783 non-banking related phishing scams, inclusive of email scams.

In the following sections, we will discuss the modus operandi of the common types of scams, modes of recovery in cases of funds diverted to Hong Kong and Singapore, and some practical tips and considerations for victims.

Modus Operandi of Common Types of Scams

Email scams

An increasing number of businesses are being targeted by very sophisticated email scams designed to deceive company employees responsible for executing financial transactions into making wire transfers (pursuant to a fake invoice or otherwise fraudulent instructions) to bank accounts controlled by the perpetrators of the scam. Fraudsters essentially hack into vulnerable email systems or use similar email addresses to give fraudulent instructions while requesting absolute confidentiality and prompt action.

Another situation which has become increasingly common throughout the pandemic is fraudsters pretending to be the victim's supplier and then directing payment to a bank account which they control. Fraudsters intercept genuine emails and claim that the payee account details have suddenly changed on account of bank-related issues and then direct the transfer of funds to an alternate bank account which they control. The unwitting

customer ends up wiring the funds to the fraudster only to later discover that their supplier had never changed its bank details and never received the said funds.

Investment scams

There are many different types of investment scams, usually involving fraudsters pretending to be successful investment managers and convincing victims to invest in their investment products or schemes. Fraudsters guarantee high returns and low risks in the beginning and later notify victims that due to market fluctuations or other issues, the investment has been lost, or that the victims have to make a further substantial sum of payment before they can withdraw or liquidate their investment. Some fraudsters use websites that mirror those of legitimate firms, or falsify transaction records to show fake profits, luring victims into investing more money. In some cases, the named companies do not even exist, making it difficult to commence legal action and to trace the funds.

Cryptocurrency scams

Unfortunately, cryptocurrency has become the new tool of choice for fraudsters given the decentralised nature and easy access of the cryptocurrency market. Similar to investment fraud scams, fraudsters generally carry out cryptocurrency scams by setting up fake websites which look remarkably similar to legitimate cryptocurrency exchange websites guaranteeing high returns and inducing victims into investing in digital currencies or transferring their cryptocurrencies into the digital wallet of the fraudsters. Once a fraudster is able to divert the cryptocurrency to a wallet they control, the victim is left with little information about the identity of the wallet holder and location of the wallet, making it very difficult to recover the funds.

Romance scams

Victims in Hong Kong reportedly lost approximately HK$600 million in romance scams in 2021 (a sharp increase from HK$212 million in 2020), while victims in Singapore reportedly lost approximately S$46.9 million in 2021, an increase of S$13.6 million as compared to 2020. In these types of scams, fraudsters often target the victim's emotional vulnerabilities and lure them into misleading relationships, only to later manipulate them into transferring funds to designated bank accounts under the pretext of a gift or a lucrative investment deal.

Key Steps for Victims of a Wire Fraud

Once the funds have been transferred to the fraudsters' bank accounts, the fraudsters tend to remove or dissipate the funds as swiftly as possible, rendering any recovery attempts futile. Time is, therefore, of the essence when it comes to tracing and recovering funds and the slightest delay on the victim's part can risk dissipation of the funds.

It is also of crucial importance to document everything relevant to the wire fraud itself, such as the emails, conversations, bank transaction details, phone numbers and email addresses. This is particularly so when the scam is perpetuated over a platform where the fraudster can delete or edit messages, such as WhatsApp or Telegram. Documentary evidence will be important whether a victim chooses to initiate civil proceedings or make a police report.

GALL

Eugene Thuraisingam LLP

HONG KONG

There are 3 important steps the victims must take immediately upon discovering the fraud when the funds have been diverted to Hong Kong:

1. Contact the bank to cancel or revert the wire transfer and request them to notify the recipient bank immediately to recall the remittance.

2. Report the wire fraud to the local police and to the Hong Kong police. The Hong Kong police have a discretion to issue a "Letter of No Consent" ("**LNC**") over the concerned bank account which serves as a temporary freeze (normally for no more than 6 months). The LNC is a very efficient and costs saving tool for the victims, but it is worth bearing in mind that the police retain the discretion to unfreeze the account anytime. The High Court of Hong Kong has recently expressed concerns over the LNC regime and held that the manner in which the police administered and maintained the LNC in that particular case disproportionately interfered with the right to the use of one's own property. In our experience, in light of the judgement, the police are now more cautious and are issuing warnings that they would lift the freeze on the accounts without further notice. This means that the victims may be forced to apply for an injunction through the Courts to prohibit the account holder from dealing with the funds which can be an expensive process.
3. Engage a fraud and asset tracing lawyer to assist with the process of recovery. Reporting the wire fraud to the police is not enough. It is also necessary to simultaneously commence civil proceedings to recover the lost funds provided the funds still remain in the concerned bank account. While the process may appear quite straightforward and something the victims can handle by themselves quite conveniently, it is not always the case. Law firms with the know-how to handle these types of claims can help prepare all the necessary Court documents, communicate with the Court and the police, and guide the victims through the process in a timely manner. If the victims are overseas, solicitors can also be the local contact so that the victims do not have to travel to Hong Kong. One thing to keep in mind is that in Hong Kong, companies must engage a lawyer to act on their behalf in court proceedings unless they obtain special permission from the Court.

SINGAPORE

If the funds have been diverted to Singapore, there are several things that can be done.

1. If the fund transfers in question are unauthorised, contact the bank immediately to report them. Though the funds are unlikely to be recovered because most fund transfers are carried out instantaneously, a funds recall may be possible under the right circumstances, sparing victims the cost and stress of pursuing other modes of recovery.

2. A victim should make a police report immediately. In recent years, the SPF has reorganised resources and set up a dedicated Anti-Scam Centre ("**ASC**") in 2019. As of 26 April 2022, the ASC has frozen more than 27,300 bank accounts and recovered more than S$200 million. The SPF's collaborations with financial institutions under Project FRONTIER (Fund Recovery Operations and Networks Team, Inspiring Effective Resolutions) have allowed them to freeze bank accounts involved in scam operations within a day from them being notified and help victims recover losses.

3. A victim can also call the National Crime Prevention Centre ("**NCPC**") at 1800-722-6688 for scam-related advice.

4. Under the right circumstances, it may be worthwhile to pursue a civil claim against the fraudster to recover losses. Whether or not this is a viable option ultimately depends on the facts of every case – for example, the likelihood that one can recover the full amount from the fraudster, whether the amounts recoverable will outweigh the costs of litigation, amongst other facts. A law firm with expertise in commercial disputes will be able to advise on the merits of the case and whether it is in the best interests of a victim to proceed.

The Monetary Authority of Singapore and the Association of Banks in Singapore have also announced additional measures to safeguard customers from digital banking scams, which are set to take full effect by 31 October 2022. These measures include an emergency self-service "kill-switch" for individuals who suspect their bank accounts have been compromised to quickly suspend their accounts. Bank staff will also be co-located at the ASC, which will help facilitate swift account freezing and fund recovery operations.

Recovery of Funds

Civil proceedings

HONG KONG

The proceedings for recovery are commenced by issuing a Writ of Summons setting out the basis of the relief sought and serving it on the defendant, i.e., the holder of the Hong Kong bank account into which the funds have been transferred.

The defendant has a short period of time to indicate whether it intends to contest the proceedings. Fraudsters often remain silent, which enables the victim of the wire fraud to apply for a default judgment.

Upon obtaining default judgment, garnishee proceedings can be commenced to enforce the judgment against the funds remaining in the bank account.

A garnishee order is obtained in 2 parts – a garnishee order nisi, which is a temporary order obtained ex parte (i.e. without notice to the bank or the defendant) on papers. Once the garnishee order nisi is obtained, the matter is set down for a short hearing at which the defendant and the bank are given an opportunity to make submissions. Unless there is a good reason why the funds in the defendant's bank account should not be attached, the Court makes the garnishee order absolute. Fraudsters often remain silent, and the bank normally does not contest the proceedings. Once the order is obtained, the bank is able to release the funds to the victim's designated bank account.

If the proceedings are uncontested, the recovery process takes approximately 6 to 8 months in straightforward cases subject to the Court's capacity.

Pursuing the individuals behind a corporate account holder is challenging as it is difficult to establish personal liability and they are likely to be in foreign jurisdictions with no identifiable assets, making both service of documents and enforcement difficult. Likewise, suing the recipient bank is not recommended as it does not owe the victim of the wire fraud any duty of care.

SINGAPORE

In Singapore, the procedure for commencing a claim for recovery against the holder of a Singaporean bank account is broadly similar, though some things have changed since the Rules of Court 2021 came into force on 1 April 2022.

After obtaining a judgment, the claimant may pursue an enforcement order under Order 22 of the Rules of Court 2021. In order to enforce the judgment against the bank account, the claimant should apply for an enforcement order for attachment of a debt. This is in essence the same as a garnishee order. Such an enforcement order will authorise the Sheriff to attach a debt due to the enforcement respondent (in this case, the defendant) from a non-party (in this case, the bank). The Sheriff will carry this out by serving a notice of attachment on the bank, in respect of the monies deposited in the account in question.

A claimant can expect the monies within about a month after service of the notice of attachment on the bank, unless the bank objects to the notice.

Injunctions

Where substantial funds are involved and have been frozen by the Hong Kong police, it is also advisable to seek an injunctive relief to prohibit the defendant from dealing with the funds in the Hong Kong bank account in view of the fact that the police may withdraw the LNC without further notice. An injunction application is required to be made promptly. Delay without a satisfactory explanation is not seen favourably by the Courts. Injunctions are costly to obtain but they do offer additional protection.

There is no equivalent to the LNC in Singapore. Under Singapore law, the SPF may seize, or prohibit the disposal of or dealing in, any property in respect of which an offence is suspected to have been committed, which is suspected to have been used or intended to be used to commit an offence, or which is suspected to constitute evidence of an offence. This includes monies held in a bank account.

In Singapore, it may also be useful in an appropriate case to seek injunctive reliefs such as a *Mareva* injunction against a fraudster to prevent the fraudster from dissipating his assets. In a situation where the fraudster has assets within Singapore, it must be shown that the claimant has a good arguable case on the merits of the claim against them, and that there is a real risk that the fraudster will dissipate assets, which would render any judgment obtained in the proceedings nugatory. The claimant must also provide full and frank disclosure of all material facts when applying for the injunction. The Rules of Court 2021 have sought to simplify the procedures involved and have consolidated the necessary steps in Order 13. Order 13 also provides that in an urgent case, injunctions can be applied for even before an originating process is issued.

Injunctions in cryptocurrency frauds

Victims of cryptocurrency fraud can also seek to apply for injunctive relief in Hong Kong, particularly if they are able to trace the transaction to a cryptocurrency exchange in Hong Kong. For example, in *Nico Constantijn Antonius Samara v Stive Jean Paul Dan [2019] HKCFI 2718 and [2022] HKCU 1899*, the Hong Kong court granted a Mareva injunction and a proprietary injunction over the assets of a cryptocurrency trader, and also granted discovery orders against the defendant to assist the plaintiff. In *Yan Yu Ying v. Leung Wing Hei [2021] HKCFI 3160*, the Hong Kong court granted an interim proprietary injunction over 999.9900261 bitcoins to preserve the subject matter of the dispute, pending substantive determination. It is worth noting that, in both cases, the Court granted the injunctions without discussing any specific issue or technical difficulties arising from the nature of cryptocurrencies.

In Singapore, *CLM v CLN and others [2022] SGHC 46* has confirmed that Singapore courts do have the power to grant injunctive reliefs, such as Mareva injunctions and proprietary injunctions, over cryptocurrency assets. This was notwithstanding the fact that at the time the injunctive reliefs were granted, the identities of the defendants were unknown. The High Court held that it would have jurisdiction over unknown person(s) as long as the description of the unknown person(s) was sufficiently certain as to identify those who do and do not fall within it.

That being said, issues regarding the identity of the wallet holder, service on the defendant, location of the wallet do arise, which increase the difficulties in the recovery exercise. Therefore, victims should act promptly in making a police report and liaising with the relevant authorities to facilitate the tracing and investigation exercise.

Tracing

The standard form of the injunction order includes a term ordering the defendant to disclose its assets, including their value and location.

Ancillary disclosure orders can also be sought against the bank as part of the injunction application.

A Norwich Pharmacal application can be made against a bank if the victim of the wire fraud does not know the identity and address of the wrongdoer but knows the relevant account number, or if the victim wants to obtain details of the status of the funds before deciding the steps for recovery. The application can be made without commencing any proceedings against the account holder. Pursuant to this application, banks can be directed to disclose bank records, such as bank account opening forms, which can help identify and locate the wrongdoer, bank statements, remittance advices. If it transpires that the funds have been transferred out, the victim may need to apply for separate disclosure orders against the next layer of recipient(s) in order to ascertain the status of those funds. The whole process can be quite expensive. Generally, a gagging order is sought against the relevant bank at the outset so that the bank is prohibited from notifying the account holder (i.e., its client) about the intended proceedings.

In ongoing civil proceedings in Hong Kong, an application under Section 21 of the Evidence Ordinance can be made against a bank to obtain bankers' records.

The Singaporean equivalent to Section 21 of Hong Kong's Evidence Ordinance is Section 175 of the Evidence Act 1893. The High Court in *La Dolce Vita Fine Dining Company Ltd v Zhang Lan and others* [2022] SGHC 89 has recently affirmed that bankers' books are limited to transactional records concerning a customer. Anything beyond that is protected by banking secrecy and not subject to disclosure.

Practical Tips to Prevent Wire Fraud

Prevention is always better than cure when it comes to wire fraud, and we set out some practical tips to prevent wire fraud:

- Regular training sessions on wire fraud and best practices.
- Never rely on a single source of instructions for payment requests or changes to payment methods.
- Double check email address, spelling mistakes in emails, and verify payment instructions by phone.
- Research before investing. Verify licenses and beware of promises of high rates of return. If the offer seems too good to be true, it probably *is* too good to be true.

In Singapore, one may protect themselves against scam messages and calls by installing ScamShield on phones running iOS. ScamShield is an app jointly built by the NCPC, the Open Government Products team at the Government Technology Agency of Singapore and the SPF. ScamShield blocks calls and filters SMSes from a database of phone numbers managed by the NCPC and the SPF.

Conclusion

To conclude, upon discovery of the fraud, victims must act immediately. They must (1) inform the banks; (2) file a police report; and (3) promptly instruct solicitors to take care of the court process. If the victims act fast and if they are fortunate, there will still be some funds left to recover. In most cases, the civil proceedings would go uncontested, and the process of recovery can be quite straightforward. The solicitors can help liaise with the bank and the police for the effective return of the funds.

Of course, each case turns on its specific facts. But the slightest of delays on the victim's part can risk dissipation of the funds, which would mean additional time and costs to trace the funds, rendering the recovery process difficult and costly.

Contacts

Gall

Kenix Yuen
Partner
kenixyuen@gallhk.com

Ashima Sood
Senior Associate
ashimasood@gallhk.com

Eugene Thuraisingam LLP

Jing Yen Chooi
Partner
jingyen@thuraisingam.com

Yuan Siang Ng
Trainee
yuansiang@thuraisingam.com