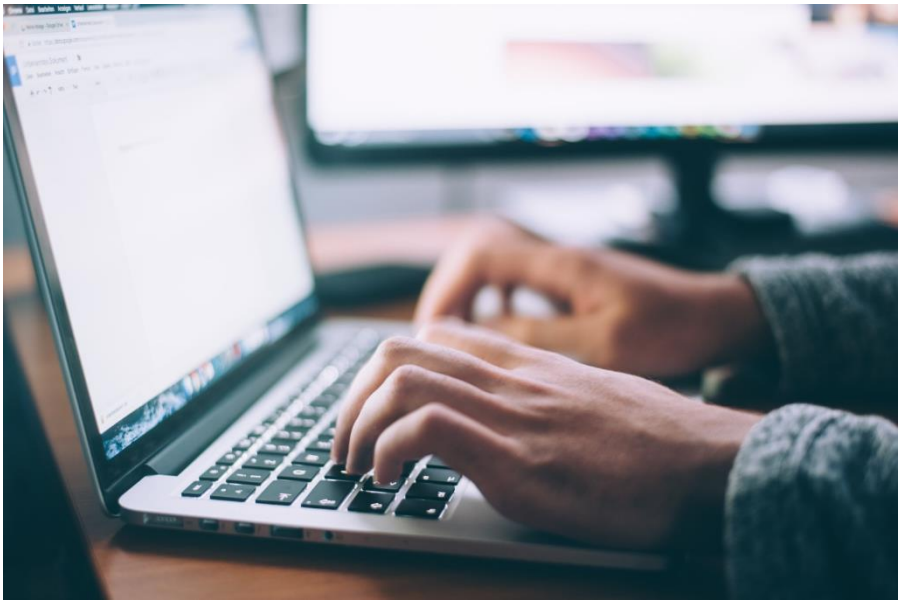
梁浩然律師事務所
有限法律責任合夥
H.Y. LEUNG & Co. LLP
SOLICITORS

H.Y. Leung & Co. LLP Quarterly Digest

Internet Fraud



by Anthony Marrin on 8 October 2020

Internet fraud: How to recover your funds in Hong Kong

Since its inception in 2017, the Anti-Deception Coordination Centre of the Hong Kong Police ("**HKP**") successfully intercepted over US$813 million that are monies stolen from victims of internet and telephone scams.

Hong Kong has unfortunately become a popular destination for fraudsters to receive and launder monies. The proceeds of fraud are often first transferred to Hong Kong, and swiftly onward paid to other bank accounts locally, or in other jurisdictions, in an attempt to make tracing and recovery implausible.

If the victim manages to react quickly, he/she may be able to intercept most (if not all) of the funds. This article provides a brief outline of how you may increase your chances of recovery.

Common trends in international internet fraud

Whilst there are still instances of the odd "Nigerian Prince" email appearing in the junk mail folder, we have seen increased sophistication in international fraud. Here are some common trends:-

"CEO" fraud: The fraudster hacks into the email of the CEO (or an officer with authority) and studies his/her practices (for example, way of communicating with others; identify vulnerable employee(s); understand travel patterns). The fraudster then impersonates the victim and fraudulently instructs the targeted employee to make payment on behalf of the company to Hong Kong, often under the guise of a *"secret deal that no one else can know about"* coupled with threats of dismissal if the instruction is not carried out immediately.

Supplier fraud: The fraudster hacks into the email of a purchaser or supplier, impersonates the supplier, and directs the victim to settle a genuine debt by paying into a designated account in Hong Kong, instead of the usual account or the account stated on the invoice.

Boiler house fraud: The fraudster sets up a fictitious investment company and introduces investment opportunities to the victim *"with guaranteed high returns"*. After receiving initial capital from the victim, the company invests and makes substantial profits (only on paper). However, when the victim demands withdrawal, he/she is often:- induced to *"invest"* more; pay service charges to secure the release; or told that the investment maybe lost unless certain monies are paid... excuses only to stall the victim and induce further payments. By the time the victim runs out of funds (or patience) the fraudster disappears.

Impersonating Government authorities: The fraudster would impersonate government officials and threaten the victim through imprisonment due to alleged unpaid taxes or involvement in criminal activities. Often the fraudster would have personal details of the victim, obtained through hacking the victim's email or social media apps.

.....

If you have been defrauded

If you have unfortunately fallen victim to an internet fraud, you may do the following:-

Inform your bank: instruct your bank to reverse the payment as the transfer may still be processing within the banking system. As long as the funds have not been credited to the target account, there is still a chance for payment to be reversed. However, once the funds have been credited to the account, the bank will not release the funds unless ordered by the Court.

Report to the Hong Kong Police: you should make a report to HKP's Cyber Crime Report Centre. The Police may issue a Letter of No Consent ("**LNC**"). The LNC acts as a *de facto* temporary freeze against the target account preventing (further) dissipation of the stolen monies. The purpose of the LNC, however, is to temporarily freeze the proceeds of crime for confiscation to the Hong Kong Government. The Police do not have the legal right or obligation to return the stolen monies to the victim.

Consult a lawyer: The bank and Police may not be able to act immediately, and even if the Police manages to issue an LNC, in any event, you need to recover the monies through issuing Court proceedings:

1. The victim can instruct lawyers in Hong Kong to apply urgently to Court for a freezing injunction and disclosure order. The freezing injunction orders the bank to stop withdrawals from the account. The disclosure order grants the victim the right to inspect the account's bank statements and trace the destination(s) of the stolen funds if they have been onward paid to 2nd level recipients (in Hong Kong or elsewhere). The victim can then instruct the lawyers to continue the tracing and recovery exercise against the 2nd level recipients, and so on.
2. Once the stolen monies have been frozen (either through the Police or the Court), the victim must take steps to recover it by taking out a civil claim against the account holder.

How we can help

Background investigation: Often the owner of recipient accounts are Hong Kong registered companies, and in certain cases, Hong Kong or Mainland Chinese

individuals. We can assist through company registry searches and investigations to identify the beneficial owners of the account.

Report / liaise with banks and enforcement agencies: We can assist international victims by reporting the fraud and our investigations to the recipient bank and HKP, and to liaise with them in providing supporting information / documents, and for withdrawal of the funds post recovery.

Experience: We have extensive experience appearing before Hong Kong High Court and District Court Judges for urgent applications for freezing injunctions and disclosure orders, and can assist the victim in all the steps towards recovery of the funds.

Global alliance: If the stolen funds have been onward transferred from Hong Kong to another jurisdiction, our firm can quickly seek assistance of member firms from Alliott Global Alliance to continue the tracing and recovery process in that jurisdiction.

READ MORE ON OUR WEBSITE