



Commercial disputes and regulatory – Hong Kong

September 2015

Faceless fraud – scams in an online world

Introduction

The internet is not necessarily a safe place. As the reliance on electronic communications in commercial transactions grows, so do the risks. As an example, in the 12 months to September 2010, the Hong Kong Monetary Authority (HKMA) published 13 press releases on fraud, mostly relating to online scams; during the past year, it has published 36 to date.

The scams reported by the HKMA include fake bank websites (24 in the past year to date) and fraudulent emails purporting to be from banks. However, this is just the tip of an iceberg. Talk to any dispute resolution lawyer in Hong Kong and you are likely to hear the same story; online fraud is rife in Hong Kong and the fraudsters often operate from overseas. Untold numbers of victims are being defrauded by scammers impersonating (for example) banks, suppliers and other businesses. There have been recent examples of some scam artists trying to impersonate Mainland security officials and a Hong Kong regulator¹.

One of the most common scams is “wire fraud”. This usually relies upon a rather simple trick – setting up an email address deceptively similar to a real address used by the victim’s supplier, which is then used to induce the victim to transfer funds to an account under the fraudster’s control. By the time the victim discovers the fraud, it may be too late to track down the funds or the criminal(s) and their associates who are responsible.

Other online scams can be more sophisticated. For example, in one recent case, a fraudster created a convincing website for a fake financial advisory service and then persuaded a victim (using a combination of online communications and telephone calls) to transfer funds to the fraudster’s bank account, supposedly to buy shares in a genuine company. The victim only discovered the fraud several months later, when he attempted to check the value of his shareholding. By that time, the money had, of course, long gone.

Any comments or queries?

Jonathan Cary Partner

+852 2216 7173
jonathan.cary@rpc.com.hk

Gary Yin Partner

+852 2216 7103
gary.yin@rpc.com.hk

Ben Yates Senior Associate

+852 2216 7169
ben.yates@rpc.com.hk

1. For example, see [SFC press release](#), 27 August 2015: “Public advised to beware of fake SFC calls offering investment opportunities”. It should be observed that, in Hong Kong, the SFC tends not to call; they are more likely to send letters and/or “Investigation Notices” or initiate court proceedings. The Police (whether in the Mainland or Hong Kong) usually prefer to “knock on the door”.

Fraud prevention

Paying close attention to the details of email communications will often reveal when something is amiss. Although there may be rare occasions when a fraudster has actually hacked into a supplier's email server and sent emails from a genuine account, usually the sender has actually created a similar domain for the bogus email account (eg, h5bc.com.hk), which will become apparent upon closer inspection. Establishing a system for email addresses to be verified by reference to existing contacts can help root out many attempted frauds.

Following up email communications with a telephone call to the supplier to confirm that it is in fact the author of those emails is usually enough to stop the fraudster in his (or her) tracks. It appears that in many of the large volume of wire fraud cases taking place in Hong Kong every year, this simple step has been neglected. Putting training and protocols in place for such identity checks, particularly before any transactions are conducted, should be a priority for any business. This is especially true for new staff who handle a business's accounts and financial affairs.

While picking up the telephone can reduce the opportunities for fraud, it also presents its own risks, as the HKMA itself knows only too well. This summer, it emerged that fraudsters had been impersonating HKMA staff members and calling members of the public to try to obtain personal information. This has prompted the HKMA to take new measures jointly with the Hong Kong Association of Banks ("HKAB") to raise public awareness of phone scams and help protect bank customers' interests, including tightening regulations on promotional calls from banks and forcing banks to offer more services for people to check callers' identities².

These examples show that no single form of communication is necessarily safe. A multi-faceted approach to fraud prevention is, therefore, needed. By using several different

means to confirm the identity of the party with whom they are dealing, individuals and corporations can significantly reduce the likelihood of falling victim to common forms of fraud. There is clearly an onus on individuals and businesses to perform their own due diligence checks.

Wire fraud – trying to get some money back

Reporting the matter

While an ounce of prevention is worth a pound of cure, if the victim discovers the fraud quickly and seeks help from experienced lawyers without delay, there may still be a chance of getting the money back, or at least some of it, before it disappears (often across borders).

First of all, it is important to contact the destination bank as soon as possible after the transfer has been made and inform them of the fraud and of the victim's claims to the money in question. Although, in the absence of a court order, the bank is unlikely to provide the victim with any information regarding the transaction, it should generally take steps to ensure that no money can be withdrawn from the account for at least a few hours. The bank will, of course, have its own internal and external lawyers and they will be concerned not to expose the bank to a claim by the legitimate owner of the funds. During these first few hours, the victim should also have time to report the matter to the Hong Kong Police.

Once a Police report has been made, depending on the facts and circumstances, the Police may send a "letter of no consent" to the bank requesting that no transfers be made from the account pending their investigations. In response to such a letter, the bank will normally temporarily "freeze" the account. The bank account may remain frozen in this manner for several days or weeks (although, there are practical limits to the duration of the freeze – an account-holder should not be deprived of the right to access legitimate funds indefinitely, when a

2. For example, see [HKAB press releases](#) – (i), 31 August 2015: "Beware of Fraudulent Calls, Verify the Caller's Identity Promotion Campaign"; (ii) 20 July 2015: "Hong Kong Banks Warn Customers Against Fraudulent Phone Calls". Also see [HKMA press releases](#).

fraud has not yet been legally established). Victims are more likely to obtain assistance from the Police in these sorts of situations when there is a group of victims and matters have a higher profile eg, they have been reported in the press. Where the alleged fraud involves a regulated entity or an entity that purports to be licensed (but is not), there are other enforcement agencies that can also assist; for example, the Securities and Futures Commission³.

Unfortunately, relying on the Police to compel a bank to temporarily freeze the recipient account is not without risk or uncertainty. It may take some time for the Police to investigate the fraud and there is no guarantee that they will ensure that the account is frozen quickly enough, or indeed at all. Matters may have also become more complicated given that the constitutionality of the Police's "no consent" regime has recently been challenged in the High Court (albeit unsuccessfully and in the context of Hong Kong's proceeds of crime legislation); it may be that the Police will become more circumspect in exercising their powers other than in the context of an active criminal investigation and a formal anti-money laundering report⁴.

Civil court proceedings

During the early "window of opportunity", the victim and their lawyers should seek to gather information regarding the bank account holder (which is usually a "shell" company with a spurious name, set up solely for the fraud), possibly with a view to commencing civil court proceedings against it. Imaginative ways may be needed to effect service of court proceedings on the proposed defendant – for example, where only the fraudster's account number (and not his/her/its name) is known, some claimants have brought proceedings against "the holder of [bank name] account number [X]"⁵. It is also worth noting that the Rules of the High Court of Hong Kong provide that where it is "impracticable" for any reason to serve (among other things) court proceedings on a defendant in the normal manner, the court may make an

order for "substituted service" – for example, by use of social media⁶.

Depending on the circumstances, it may be necessary to apply to court for an order compelling the bank to disclose the account-holder's details. Sometimes, it may also be necessary to escalate matters by including the bank as a party to the court proceedings.

If there is a large amount of money at stake, or if the Police do not take immediate steps to freeze the account, the claimant may need to apply to court for a "Mareva injunction", freezing the destination account. This is a more formal, and more costly, court-ordered freeze on the bank account, which can be obtained relatively quickly and give a claimant time to investigate and pursue a bona fide claim against the fraudster and/or their associates. However, as readers will appreciate, obtaining such a court order comes with significant responsibilities and cost.

In most cases, the bogus shell company will do nothing in response to the court proceedings and the claimant can proceed to a "judgment in default" against it within a few weeks. That "judgment in default" (once obtained) can be used to obtain a "garnishee order", pursuant to which the bank can be ordered to pay funds from the fraudster's account back to the claimant. In more complex matters, where a claimant asserts proprietary rights and seeks to recover more than just a debt, the court proceedings will take longer. If there is enough money in the account, the claimant can also seek to recover some of the legal costs involved in pursuing the claim.

In some circumstances, the fraud victim may have the option to bring a claim against their own bank, usually for "breach of mandate" or for failing to have adequate controls and systems in place to identify suspicious transactions and ensure compliance with anti-money laundering rules. Such claims may arise, for example, where the victim's

3. For example, see [SFC's "Alert List"](#).
4. *Interush Ltd v Commissioner of Police* [2015] HKEC 1589 (in the context of s. 25A(2)(a) of the *Organized and Serious Crimes Ordinance*) and pending likely appeal to Court of Appeal.
5. For example, see High Court Action No. 913 of 2015, commenced on 27 April 2015.
6. RHC Order 65, rule 4.

bank, having been notified of the fraud or of suspicions regarding the recipient account, still allows a fraudulent transfer to go through, or where the bank has given effect to fraudulent transfer instructions purportedly given on behalf of the victim. More rarely, the victim may be in a position to take action against the fraudster's bank for compliance failings, such as breaches of "know-your-client" rules.

Many of these types of frauds and scams, while often carried out by relatively simple means, lead to complex legal issues, such as – banking secrecy and disclosure, freezing and recovering funds from bank accounts, dealing

with foreign jurisdictions (since the fraudsters generally do not delay in transferring the money overseas), tracing assets and the practical difficulties of dealing with the Police, banks and other institutions quickly and effectively.

Commencing civil proceedings, alongside a criminal and/or regulatory investigation, can be effective but requires resourcing; not to mention careful and expeditious judgement. If you have fallen victim to online fraud, engaging a law firm with experience in dealing with such matters can help make the difference between recovering your money (or at least some of it) and losing it.

This Smyth & Co in association with RPC article is intended to give general information only and may be of general common law interest. It is not a complete statement of the law. It is not intended to be relied upon or to be a substitute for legal advice in relation to particular circumstances. Written by Ben Yates (assisted by Warren Ganesh).

For regulatory reasons, RPC operates as a registered foreign law firm in Hong Kong and in association with Smyth & Co.

About RPC

RPC is a modern, progressive and commercially focused international law firm. We have 78 partners and over 600 employees based in London, Hong Kong, Singapore and Bristol.

"... the client-centred modern legal services business."

At RPC we put our clients and our people at the heart of what we do:

- Best Legal Adviser status every year since 2009
- Best Legal Employer status every year since 2009
- Shortlisted for Law Firm of the Year for two consecutive years

We have also been shortlisted and won a number of industry awards, including:

- Winner – Law Firm of the Year – The Lawyer Awards 2014
- Winner – Law Firm of the Year – Halsbury Legal Awards 2014
- Winner – Insurance and Reinsurance Law Firm of the Year, Hong Kong - Finance Monthly Law Awards 2015
- Winner – Hong Kong - Leading Litigation Lawyer of the Year - ACQ Global Awards 2015
- Nominated - Maritime and Shipping Law Firm of the Year - Hong Kong - Lawyer Monthly Legal Awards 2015
- Winner – Commercial Team of the Year – The British Legal Awards 2014
- Winner – Competition Team of the Year – Legal Business Awards 2014
- Winner – In-House Community Firm of the Year, Hong Kong Insurance - Asian-Mena Counsel 2013
- Highly commended – Law Firm of the Year at The Legal Business Awards 2013
- Highly commended – Real Estate Team of the Year at the Legal Business Awards 2013

"... they are my firm of choice in Asia." Chambers Asia Pacific 2015

Areas of specialism

- | | | |
|-------------------------|----------------------------------|---------------|
| • Banking | • Insurance | • Real Estate |
| • Commercial | • Intellectual Property | • Regulatory |
| • Commercial Litigation | • International Arbitration | • Reinsurance |
| • Competition | • Marine and International Trade | • Tax |
| • Construction | • Media | • Technology |
| • Corporate | • Outsourcing | |
| • Employment | • Private Equity | |

