Handbook on Financial Frauds and Action to be taken by victims in HKSAR 2023

Introduction

Hong Kong, China is one of the leading international financial centers and is also a free port where a free trade policy is pursued with no barriers on trade. A large number of trade transactions are undertaken in Hong Kong, which include genuine trade transactions as well as a number of fraudulent transactions conducted by dummy companies operating within the jurisdiction of Hong Kong, China.

Since the outbreak of the COVID-19 pandemic, there has been a drastic increase in cyber fraud cases involving email wire fraud scams and phone scams around the world. There has been significant increase in cases wherein fraudulent emails and WhatsApp messages have been sent to induce victims into clicking malicious links or opening attachments.

This handbook aims to provide comprehensive information to victims on dealing with frauds in general and business frauds in particular, where the fraudster is based in the jurisdiction of Hong Kong, China.

To pursue a case of fraud in Hong Kong the following actions are recommended:

(A) Report to law enforcement authorities
(B) Initiate Civil Action
(C) Police Investigation in Hong Kong
(D) Police Investigation in India

The first and foremost action that needs to be taken in the case of a fraud is to stop the movement of funds. The Hong Kong Police Anti Deception Center (ADCC) helpline can help a victim in this regard. The ADCC will take the request for instructing the recipient bank to stop movement of funds **only if** the following conditions are met:

a) The victim files an FIR in India with facts establishing there is an element of fraud and no commercial dispute
b) The victim provides all the details of the transaction at the atomic level
c) The amount transferred is more than 100,000 HKD
d) The amount was transferred within a week.

If any victim can satisfy the above criteria then he is advised to approach ADCC directly. The victim may share the information with the Consulate General of India, Hong Kong (CGIHK) for information. **Please note that the CGIHK will not be in a position to take any action in relation to the complaint lodged with the ADCC**.

In other cases, the victim should report the case to the e-Report center of the Hong Kong Police. Once a case is reported to the e-Report center, the case is assigned to a district for investigation. The case officer will reach out to the victim. The victim may share the information with the Consulate General of India, Hong Kong (CGIHK) for information. **Please note the CGIHK will not be in a position to take any action in relation to the complaint**

lodged with the e-Report center.
In cases where there is no element of fraud but the dispute is purely a commercial dispute, the institution of a Civil suit by the victim is the preferred course of action.

Cyber Frauds

Cyber frauds are mainly conducted over the internet. Money is transferred from the victim's bank account(s) in India to a fraudster's bank account(s) in Hong Kong, China. These frauds can cause severe financial losses to businesses. Below are some common types of fraud:

Sale contract scam/corporate scam

Fraudsters impersonate the parties to the contract by using the same email account or similar domain account. For instance, fraudsters impersonate sellers and send fictitious emails to the victim buyers, claiming that the sellers' bank account has changed and request transfer of funds to other bank accounts which are operated by the fraudsters.

CEO scam

Fraudsters pretend to be senior management officials of the company and request employees to transfer the company funds to the bank accounts controlled by the fraudsters.

Business Email Compromise

Criminals hack into email systems or use social engineering tactics to gain information about corporate payment systems. They then deceive company employees into transferring money into their bank account.

E-Banking Fraud

When victims log into their online banking accounts on the Internet, fraudsters make use of computer technology to display a series of bogus web page interfaces on victims' computers that entice the victims to input important information (such as login name, password and one-time password issued by a security device). Then the fraudsters will use the above gathered information (including one-time password) to complete the double authentication process, and cheat money out of the victims through online banking transfers.

Social Media Deception

Swindlers log into social media accounts with login names or email addresses and passwords acquired by illegal means. They then pose as the users of these accounts and send deceptive messages to the users' friends on the contact lists, requesting them to buy virtual point cards or reload cards on their behalf. They also ask for the serial numbers/authorization codes and passwords on the cards. Having fraudulently obtained this information they then cannot be reached thereafter.

Report

Victim Bank

The first step to fight fraud and recover the funds is to report the fraud to the victim bank. Once the funds have been transferred to the fraudsters' bank accounts, the fraudsters will remove the funds as quickly as they can, rendering the subsequent recovery of the funds futile. Hence, victims should contact their banks about the fraudulent incident and request them to notify the recipients' banks and request cancellation, recall or reversal of the remittance. Banks can alert each other to the suspected fraudulent activities. They usually freeze the recipients' bank accounts temporarily pending their internal investigation.

Fund Recall Request

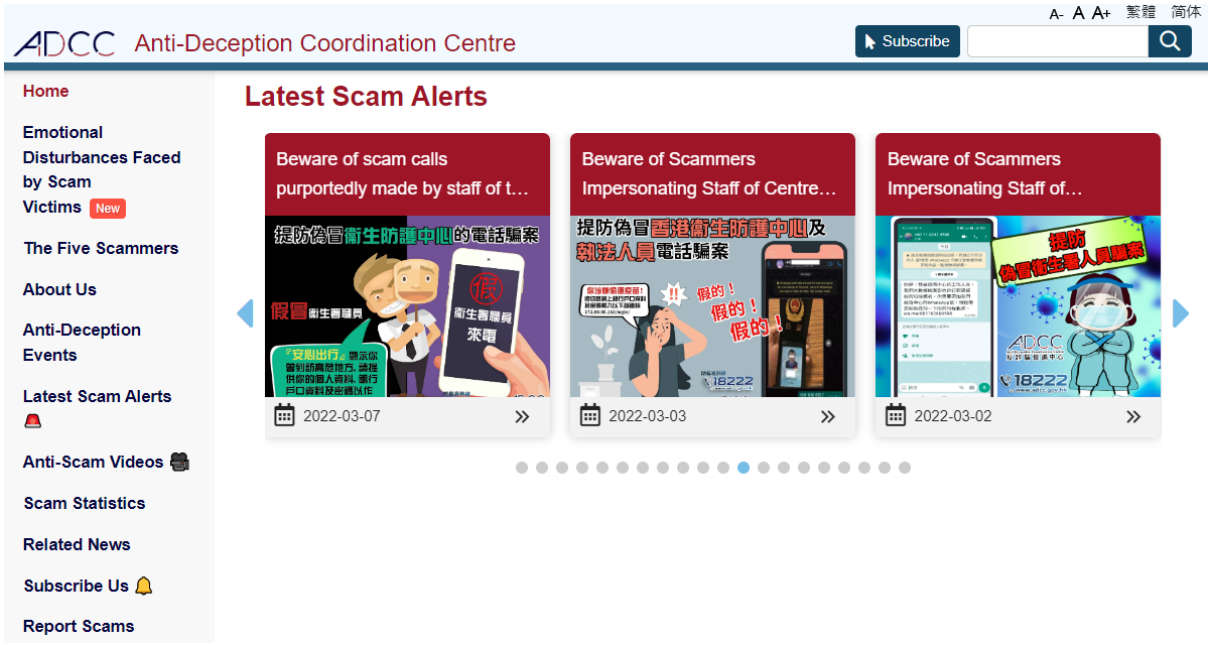
The victim should approach their bank to issue a fund recall request. This is very important in cases where the victim reports the incident within 24 hours of the incident. There is a possibility that the recipient bank will honor the fund recall request.

Even otherwise, it is recommended that the victim gets in touch with their bank to issue a fund recall request. **Hong Kong Police will request a copy of the fund recall request in their investigation**.

Anti-Deception Coordination Center

Hong Kong Police established the Anti Deception Coordination Center (ADCC) in July 2017 to step up action against deception and enhance public awareness of various kinds of scams. Frauds that fall in the category of deception can also be reported to the Anti Deception Coordination Center (ADCC). Through the “Anti-Scam Helpline 18222” hotline, the Anti-Deception Coordination Centre of the Hong Kong Police Force provides anti-deception consultation services around the clock.
The general public can dial (+852 18222) to contact the ADCC officers for assistance in response to suspicious deception cases. The hotline also provides the latest modus operandi of deception and scam alerts, in order to respond to the topical scams in an effective manner.

Visit https://www.police.gov.hk/ppp_en/04_crime_matters/adcc/ for Latest Scam Alerts



The Anti Deception Coordination Center Hotline will be able to take the request for stopping the movement of funds in the recipient bank account if the Victim provides a copy of First Information Request (FIR) and the details of the transaction (at transaction level).

Please note: The ADCC can issue a stop request to the recipient bank only when the following conditions are met:
(i) Amount is more than HK$100,000; and
(ii) the amount was transferred within a week.

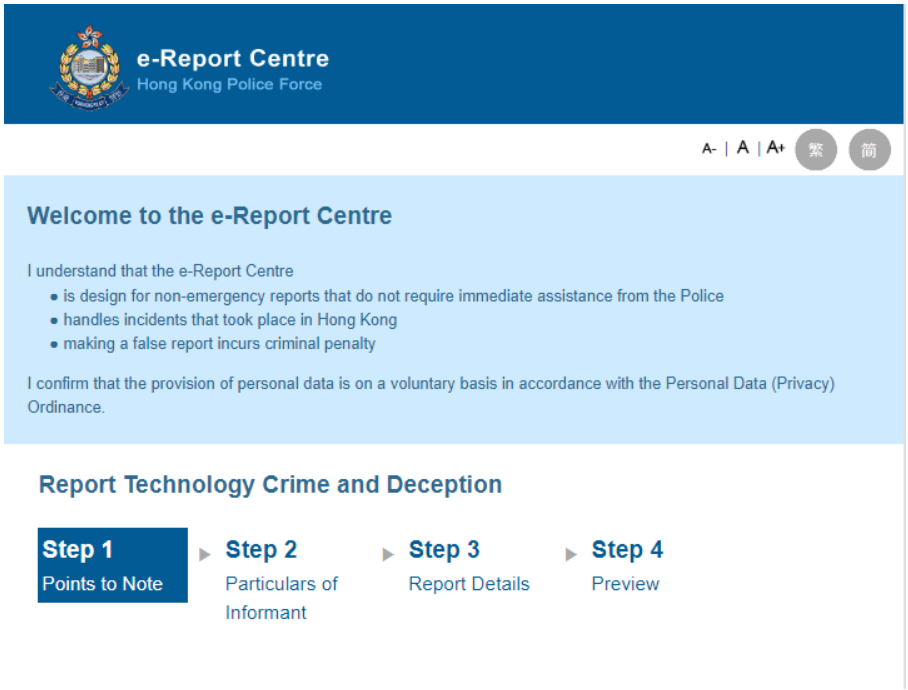
In case the fund stop request is successful, the ADCC will inform the victim and the Crime Record Bureau will assign the case to the district for investigation. The investigation officer will get in touch with the Victim.

The only outcome of the ADCC is a successful fund stop request in case of urgent cases. The case is ultimately marked to the district for investigation. The ADCC will generate a reference number for tracking of the case.

e-Report Center

A cyber crime can be reported to Hong Kong police via e-Report Center. The e-Report center takes the report and the report is forwarded to the Criminal Record Bureau which in turn assigns the case to the district for investigation.

Visit the e-Report Centre of Hong Kong Police Force at
https://www1.erc.police.gov.hk/cmiserc/EGIS-HK-Web_NEW_UI/ereport_details?report=TCAD&fontSize=100&vTimeoutReminder=1740000&vTimeoutVal=1800000&vTimeoutReminderVal=60000



Fill in the e-report form on e-Report Centre by providing the following information:

- Particulars of Informant
- Name (in English or Chinese)
- Phone Number.
- Identification Document No. & Place of Issue
- Email Address
- Correspondence address
- Are you the victim of this Cyber Crime?
- Brief Facts of Case
- Date and Time of Offence
- Location of the Crime
- Brief description of the incident
- Hyperlink of the subject Website (If applicable)
- Details of the suspect(s) or company(ies) (Company Name, address, email, contact no, address etc.)
- Financial loss (If applicable: Please state the details of the first transaction including the bank name, account number and amount involved etc.)
- Supporting document or images (email/ bank slip/invoice)

The only outcome of the e-Report center is the successful reporting of the crime. The case is ultimately marked to the District for investigation. The e-Report center will generate a reference number for tracking of the case.

Bank

The victim can also reach out to the fraudster's bank(s) and report the fraud. Though the bank is not obligated to take any action it may help the victim to alert the bank about the suspected account. The bank hot line numbers are provided in the Annexure.

Civil Action

Mareva injunction

As soon as the victims are aware of the fraudulent transfers, they should through their solicitors apply to a court in Hong Kong for an injunction order to prevent the recipients from dissipating the assets before a judgment is obtained against them.

To apply for a Mareva injunction, the plaintiff shall show to the court that:

- there is a good arguable case on a substantive claim against the defendant;
- the defendant has assets within Hong Kong;
- the balance of convenience is in favour of granting this injunction order; and
- there is a real risk of dissipation or secretion of assets by the defendant before the court can make the final judgment at the coming trial.

Proprietary injunction

A proprietary injunction is to preserve assets to which the plaintiff has a proprietary claim. If the plaintiff has been induced to transfer funds by fraud, the recipient may hold such funds on constructive trust for the plaintiff. As compared with the Mareva injunction, the threshold for obtaining a proprietary injunction is lower than obtaining a Mareva injunction that the plaintiff only has to show a serious issue to be tried on the merits. There is no need to prove there is a real risk of dissipation of assets by the defendant as is required for a Mareva injunction.

Disclosure in aid of the Mareva injunction

The standard form of the Mareva injunction allows the court to order the defendant to disclose his assets, including the value, location, and details of all these assets, so as to allow the plaintiff to know the existence, nature and location of assets. However, this information does not reveal whether the defendant has dissipated the assets, and if so, the whereabouts of the assets. In this circumstance, the plaintiff may have to apply for a bankers trust order against the defendant' s bank. In addition to injunction and disclosure applications, the victim can prefer other civil suits to recover the funds.

Please note the CGIHK will not be in a position to advise for selection of a Lawyer / Solicitor for taking up the Civil Suit.

Police Investigation in Hong Kong

The incidents which are reported either to ADCC or e-Report center are in turn processed by the Criminal Record Bureau of Hong Kong Police. The case is then in turn assigned to the District for investigation. Other than stopping the fund in the recipient bank no outcome is achieved at this stage.

The investigating officer will get in touch with the victim and inform that the case has been assigned to him. The investigating officer will also suggest to the victim that he can pursue the course of civil action.

The investigating officer will request for a witness statement to begin the investigation. It is advisable that the victim prepare a draft statement and forward to the investigation officer with all relevant information. It is recommended to keep ready the information which is required to be reported to the e-Report center along with the statement. The key information which is required to be provided to the investigation officer are:

- Classification of fraud
- Amount involved in the fraud
- Indian Bank and Hong Kong Bank
- Bank Account numbers
- Name of the beneficiary
- Details of the transaction
- **FIR in India** and
- **Fund recall request**.

The purpose of a witness statement is to establish an element of fraud. If the investigating officer does not find the element of fraud in the case, then the matter will be closed. Further the investigating officer would want to confirm the victim's willingness to testify at any future trial, if any.

It is advisable that the victim confirms that he/she provides his / her consent to pursue the case. The victim may also consent that he / she can testify through video link without the need to visit Hong Kong for the case.

Please note without the consent, the investigating officer will not investigate the case. In case the investigating officer finds no element of fraud or no consent to pursue the case, then there will be no investigation by the Hong Kong Police. The only recourse remains is to take civil action.

Police Investigation in India

The victim can also pursue the matter with the investigation authority in India. In case the investigation authority in India deems fit they can request assistance from Hong Kong's Central Authority (Department of Justice) under the "Mutual Legal Assistance Treaty on Criminal Matters" between Hong Kong, China and India.

FAQ

If I receive calls from Hong Kong's banks, how can I verify the identity of the caller?

The Hong Kong Association of Banks and the DTC Association has issued 'Code of Practice' (CoP) on Person-to-Person Marketing Calls. According to the Cop, the major retail banks engaging in telemarketing activities have agreed that their telemarketers will now provide the called person with the telemarketers' specific identity information, such as staff ID, direct line or phone extension in addition to the current requirements. The public can then call the bank's hotline below to verify the identity of the caller.

List of hotlines for authenticating the identity of callers claiming to be bank representatives is as below:-

Retail Banks	Hotline Numbers
Airstar Bank Limited	3718 1818
Ant Bank (Hong Kong) Limited	2325 0303
Bank of China (Hong Kong) Limited	3988 2388
Bank of Communications Co., Ltd.	2239 5559
The Bank of East Asia, Limited	2211 1388
China Construction Bank Corporation	2779 5533
China Merchants Bank Co., Ltd.	3118 8888
Chiyu Banking Corporation Ltd.	2843 0111
Chong Hing Bank Limited	3768 6888
Citibank (Hong Kong) Limited	2860 8888
CMB Wing Lung Bank Ltd.	2309 5555
Dah Sing Bank, Ltd.	2828 8168
DBS Bank (Hong Kong) Limited	2290 8888
Fubon Bank (Hong Kong) Limited	2566 8181
Fusion Bank Limited	2111 2688
Hang Seng Bank Ltd.	2822 0228
The Hongkong and Shanghai Banking Corporation Limited	2233 3000
Industrial and Commercial Bank of China (Asia) Limited	3510 8888
Livi Bank Limited	2929 2998
Mox Bank Limited	2888 8228
Nanyang Commercial Bank, Ltd.	3982 9960
OCBC Wing Hang Bank Limited	2815 5211
Ping An OneConnect Bank (Hong Kong) Limited	3762 9900
Public Bank (Hong Kong) Limited	2541 9222
Shanghai Commercial Bank Ltd.	2818 0282
Standard Chartered Bank (Hong Kong) Limited	2886 8888
Welab Bank Limited	3590 6396
ZA Bank Limited	3665 3665

Where can I obtain additional information about using the Internet Banking and Mobile Banking safely?

- The Hong Kong Monetary Authority:
  Internet Banking - Keeping your money safe
  Smart Tips on Using Self-banking Services
  Smart Tips on Using Internet Banking Services
  Smart Tips Against Phishing Emails
- The Hong Kong Association of Banks:
  Internet Banking - Convenient & Safe
  Beware of Phishing Websites
- Hong Kong Police Force:
  One-stop cyber security information website
  Email scam and IT security tips to mitigate the risk of hacking

- HKSAR:

The Government's Cyber Security Information Portal
The InfoSec Website

- HKCERT:
  Security Guideline

Thank you for your attention. This booklet is only an advisory.