

For discussion  
on 1 June 2021

**Legislative Council Panel on Security  
Initiatives for Preventing and Combatting  
Deception Cases**

**Introduction**

This paper introduces the work of the Police in preventing and combatting common types of deception, including online shopping scams, email scams, investment scams and telephone deception.

**Background**

2. Deception is a serious offence. Any person who commits the offence of fraud under section 16A of the Theft Ordinance (Cap. 210) is liable to imprisonment for up to 14 years, while any person charged with obtaining property by deception under section 17 of the same Ordinance is liable to imprisonment for up to 10 years. In addition, any person charged with dealing with property known or believed to represent proceeds of indictable offences under section 25 of the Organized and Serious Crimes Ordinance (Cap. 455) for proceeds of deception is liable to imprisonment for up to 14 years and a fine of HK\$5,000,000.

3. The number of deception cases has shown an upward trend over the past five years from 2016 to 2020. In 2020, the number of cases further rose to 15 553 following a year-on-year increase of nearly 90%, accounting for a quarter of the overall crime figures. Victims incurred losses totaling over HK\$3.5 billion. In the past five years, over HK\$13 billion were involved in deception cases, most of which were transferred to offshore accounts by fraudsters and syndicates within a short period of time and were difficult to trace. One of the main reasons for the significant rise in the number of deception cases was that in light of the social distancing and work-from-home arrangements etc. during the COVID-19 pandemic, people stayed at home to shop and make friends using the Internet and social media, making themselves more susceptible to various types of deception.

4. These scams are usually of transboundary and transnational nature, involving overseas criminal syndicates or with payment transferred overseas. In the past, Police have taken joint operations with law enforcement agencies of different jurisdictions, including the Mainland, Macau, Singapore, Malaysia and Spain, cracking down multiple scam syndicates mainly involving in telephone and email scams.

**Common types of deception**

*Online shopping scams*

5. There were 1 461 online shopping scam cases in the first quarter of 2021, incurring losses closed to HK\$18 million. The number of online shopping scam cases and the amount of losses in the past five years are tabulated below:

	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Number of cases</b>	1 302	1 663	2 187	2 194	6 678
<b>Amount of losses (\$ million)</b>	27.5	29.7	50	27.3	122.3

	<b>1<sup>st</sup> quarter of 2020</b>	<b>4<sup>th</sup> quarter of 2020</b>	<b>1<sup>st</sup> quarter of 2021</b>
<b>Number of cases</b>	2 439	1 357	1 461
<b>Amount of losses (\$ million)</b>	62.5	22.3	17.8

6. Online shopping has become more common during the pandemic, leading to a larger increase in the number of related deception cases. In 2020, there were 2 538 deception cases related to online purchase of face masks, accounting for almost 40% of the overall number of online shopping scams.

7. The Police took proactive enforcement actions targeting the rising trend of deception cases related to online purchase of face masks. A total of 150 persons involving in at least 440 cases were arrested during the year. The Police have also, through different channels, especially online publicity, reminded the public to be more vigilant when conducting online transactions. To reduce the risks of online shopping scams, the Police have tightened cyber security to combat malicious domains and remove a number of locally registered phishing websites as well as botnet domains (of which at least 170 were themed around COVID-19).

#### *Email scams*

8. Email scams have reflected a fluctuating trend over the past five years. There were fewer cases in the first quarter of 2021 when compared with the same period last year and the previous quarter, but the amount of losses was higher than that of other types of online scams. The number of email scam cases and the amount of losses in the past five years are tabulated below:

	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Number of cases</b>	883	693	894	816	767
<b>Amount of losses (\$ million)</b>	1,783.7	993.1	1,716.9	2,535.5	2,247.4

	<b>1<sup>st</sup> quarter of 2020</b>	<b>4<sup>th</sup> quarter of 2020</b>	<b>1<sup>st</sup> quarter of 2021</b>
<b>Number of cases</b>	230	153	145
<b>Amount of losses (\$ million)</b>	867	372.9	482.8

9. Fraudsters will hack into the email systems of companies or individuals to monitor their business dealings or correspondences. Subsequently, they will impersonate the senior staff, business partners, relatives or friends of the victims, and send fraudulent emails to instruct the victims to make payment to designated bank accounts. In 2020, the highest amount of loss in a single email scam was HK\$314.04 million.

10. To combat cross-boundary email scam syndicates, the Police proactively exchange intelligence with overseas law enforcement agencies. In 2020, the Police conducted joint law enforcement operations with the law enforcement agencies of Singapore and Macau. The Anti-Deception Coordination Centre (“ADCC”) of the Police also

strengthens collaboration with local and overseas organisations to enhance their capability in intercepting fraudulent payments, so as to minimise the loss of victims.

*Investment scams*

11. In the first quarter of 2021, the number of investment scam cases had shown a substantial increase over the same period last year and the previous quarter, involving losses totaling over HK\$1.9 billion. The number of investment scam cases and the amount of losses in the past five years are tabulated below:

	<b>2016</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>
<b>Number of cases</b>	134	137	212	300	510
<b>Amount of losses (\$ million)</b>	602	158.7	1,767.7	1,249.7	856.1

	<b>1<sup>st</sup> quarter of 2020</b>	<b>4<sup>th</sup> quarter of 2020</b>	<b>1<sup>st</sup> quarter of 2021</b>
<b>Number of cases</b>	62	200	297
<b>Amount of losses (\$ million)</b>	55.1	625.6	1,935.2

12. In recent years, fraudsters have often engaged victims via social media platforms, going so far as to gain their trust by asking after them in a charming disguise. The fraudsters will then lure them into making all kinds of investment that are falsely claimed to be of high return and low risk, or even of capital preservation. At the end, the victims often will not get any return from their investment but lose all their capital before long. Some fraudsters will give the victims a small amount of money at first, faking it as a return, so as to tempt them to boost their investment capital, and eventually cheat them of all their capital and returns.

13. Fraudsters use a wide range of investment tools as a cover for fraud, from financial products, businesses in partnership, commodities, foreign exchange, overseas properties to virtual currencies that have emerged in recent years. Among all investment fraud cases in the whole year of 2020 and the first quarter of 2021, those involving virtual currencies accounted for about 45% and 55% respectively.

14. The Police have been striving to fight against investment fraud. From 2020 to March 2021, the Police detected 58 cases with an aggregate loss of over HK\$2.332 billion and arrested 181 persons. The Police will continue to closely monitor the crime trends, and provide information on the latest deception to the public through channels such as the Police's social media platforms, the ADCC's webpage, press conferences, anti-fraud seminars, television and radio programmes, as well as community publicity events.

*Telephone deception*

15. Telephone deception, once under control in 2018 and 2019, developed an

upward trend again in 2020. The number of cases in the first quarter of 2021 was higher than that of the corresponding period last year, and the amount of losses increased substantially. The number of telephone deception cases and the amount of losses in the past five years are tabulated below:

	2016	2017	2018	2019	2020
<b>Number of cases</b>	1 138	991	615	648	1 193
<b>Amount of losses (\$ million)</b>	221.6	229.4	60.9	150	574.8

	1 <sup>st</sup> quarter of 2020	4 <sup>th</sup> quarter of 2020	1 <sup>st</sup> quarter of 2021
<b>Number of cases</b>	169	298	200
<b>Amount of losses (\$ million)</b>	54.2	170	352.6

16. The prevalent modi operandi of telephone deception are “Pretend Officials” and “Guess Who”. In “Pretend Officials” cases, fraudsters will often pose as government officials, staff members of logistics companies or other public or private organisations. They will call the victims and alleged that they are involved in criminal cases in the Mainland. The calls will then be diverted to their accomplices, who will pretend to be a “Mainland official” for swindle. In “Guess Who” cases, fraudsters will call and ask the victims to guess their identity. Once the victims respond, they will impersonate the victim’s relative or friend for swindle.

17. In 2020, “Pretend Officials” cases accounted for about 57% of all telephone deception cases. Among the 652 victims suffering monetary loss in “Pretend Officials” cases, 45% were aged 30 or below, about 30% were aged 61 or above, and about 30% were new immigrants and new arrivals who came to Hong Kong to study, work and visit relatives. As to the 498 victims suffering monetary loss in “Guess Who” cases, about 60% of them were aged 61 or above.

18. Most telephone deception cases involve cross-boundary criminal activities. Apart from cross-boundary telecommunication services, fraudsters also use local anonymous pre-paid subscriber identity module (“SIM”) cards (“PPS cards”) to place calls to victims, handle the money received or open “stooge bank accounts”, making it more difficult for the Police to investigate. In this regard, the Government completed earlier this year a public consultation, and is making new regulations under the Telecommunications Ordinance (Cap. 106). The new regulations seek to implement the Real-name Registration Programme for SIM Cards to plug the current loophole caused by the anonymous nature of SIM cards, especially PPS cards, and facilitate the prevention and detection of crimes related to the use of PPS cards, thereby maintaining people’s confidence in the integrity of the telecommunication services in Hong Kong.

19. The Police have been combating deception with Mainland and overseas law enforcement agencies. In 2019 and 2020, the Police, together with 32 countries and regions

from around the world, took part in “Operation FIRSTLIGHT”, a joint exercise against telephone deception and social media scams coordinated by the International Criminal Police Organization (“InterPol”). The Police also assisted in coordinating related joint meetings, exchanged work experience and discussed the way forward to combat deception with law enforcement officers from different places.

20. The Police continue to analyse modus operandi and trends of deception, while strengthening the preventive and educational measures. Apart from enhancing publicity through traditional channels, the Police have, in recent years, mapped out a broad variety of promotional strategies for preventing telephone deception among specific target groups. For instance, the Police have widely made use of social media, arranged exchanges with the banking sector and money services sector, and collaborated with social services agencies.

### **The ADCC**

21. To comprehensively coordinate Police resources, enhance collaboration with various stakeholders, reinforce the combat against deception and raise the public’s anti-deception awareness, the Police’s Commercial Crime Bureau established the round-the-clock ADCC in 2017. The ADCC performs duties including -

- (a) managing and operating the 24-hour “Anit-Scam Helpline 18222” to facilitate public enquiries and provide timely assistance;
- (b) cooperating with the banking sector and overseas law enforcement agencies to intercept payments to fraudsters, so as to minimise the victims’ loss;
- (c) mounting intelligence-led law enforcement operations;
- (d) clamping down on fraud through proactive collaboration with relevant stakeholders; and
- (e) coordinating anti-deception publicity work.

22. From its inception till March 2021, the ADCC received more than 80 000 telephone enquiries from members of the public. Staff of the ADCC proactively provide anti-deception advice to callers, and assist those in need to make a report. The ADCC had timely detected 1 012 ongoing deception cases and persuaded the victims not to make payments to the fraudsters.

23. The ADCC has been actively cooperating with the local banking sector to intercept payments to fraudsters so as to minimise the victims’ loss. In October 2019, it set up the “International Stop-Payment Mechanism” with the Financial Crimes Unit of the InterPol to enable most member states to make mutual stop-payment requests, thereby facilitating the Police to combat cross-border deception more effectively. From its inception till March 2021, the ADCC has successfully intercepted more than HK\$7.85 billion in 2 170 deception cases where payments had already been made to local and overseas banks.

24. The ADCC closely monitors deception cases in the territory, analyses crime trends and coordinates the anti-deception operations of various police formations. From its inception till March 2021, the ADCC conducted 364 operations with frontline police formations, with 392 people arrested and another 17 intercepted in 465 deception cases. Moreover, it set up the Intelligence and Scam Response Team in October 2020 to analyse the money-laundering networks related to deception cases, and crack down on deception-related money-laundering activities through law enforcement operations.

25. Deception and crimes related to money-laundering have no geographical boundaries. Full cooperation among overseas and local stakeholders is important in combating them. The ADCC timely disseminates information about deception and money-laundering to relevant overseas law enforcement agencies through a close police cooperation mechanism, so as to enable them to take corresponding actions. From time to time, the ADCC also shares with local banks measures and strategies for combating deception and money-laundering, and encourages the banking sector to effectively deal with suspicious accounts that handle fraudulent payments by conducting customer due diligence more cautiously and using technology appropriately.

26. To raise the public's anti-deception awareness, the ADCC analyses the trends of various types of deception cases and the profile of victims, coordinates with various police formations to formulate comprehensive anti-deception publicity strategies, and conducts crime prevention publicity among different target groups through various platforms, including the social media of the Police, the webpage of the ADCC, public transport, landmark buildings, mass media etc. The Police created an anti-scam mascot "The Little Grape" (its Chinese name is an abbreviation, meaning to be mindful of scammers) in mid-2020 in a bid to disseminate causal and simple anti-scam messages to members of the public, and encourage them to spread the same to their relatives and friends.

### **Way Forward**

27. As various types of deception involve fraudsters and criminal syndicates using internet or messaging applications to lure victims into scams, the Police are actively exploring the use of technologies to provide automatic alerts to victims when fraudsters make the first contact, so as to remind victims to carefully identify senders of emails and messages and avoid being scammed.

### **Conclusion**

28. Combating "Quick Cash Crime" continues to be one of the key operational areas set out in the Commissioner's Operational Priorities 2021. The focus of work in this regard includes targeting criminal groups involved in deception through joint efforts with stakeholders under the support of the ADCC, enhancing public awareness and securing community support to prevent "quick cash crimes", particularly telephone deception, internet and social media scams. The Police will continue to enhance public awareness and combat all types of deception through strengthening law enforcement, publicity and education, multi-agency cooperation, intelligence analysis and cross-boundary collaboration. The Police appeal to members of the public to stay alert at all times so as to avoid becoming fraudsters' target. Suspected cases of practicing deception or falling prey to deception should be reported to the Police for follow-up or to the "Anti-Scam Helpline 18222" for enquiry.

**Security Bureau**  
**Hong Kong Police Force**  
**May 2021**