LCQ20: Protecting consumers' rights and interests of online shoppers

Following is a question by the Hon Paul Tse Wai-chun and a written reply by the Secretary for Commerce and Economic Development, Mr Edward Yau, in the Legislative Council today (May 16):

Question:

Recently, some members of the public have complained that allegedly deceptive online shopping advertisement pages, which offer high-priced authentic commodities (e.g. famous brand headsets, electronic game players, video recording equipment, intelligent robots, sneakers and pricey jewellery) for sale at low prices, are prevalent on the social media platform Facebook. It is learnt that such pages mostly use "closure of physical shops", "presence of defects in the commodities" or "detention of goods by the customs and excise authorities" as a pretext for commodities being sold at prices as low as about 10 per cent or 20 per cent of the original prices, and are uploaded with captured images of bills to prove the authenticity of the goods concerned, which lured members of the public to rush to place purchase orders. Some of the pages even use the addresses of shops selling authentic goods as collection points in order to dull the vigilance of members of the public. However, members of the public who had made payments for the purchases found out that (i) they had been defrauded only when they went to pick up the goods at the relevant addresses, or (ii) the goods did not match the descriptions only after they had unwrapped the package of the goods delivered by couriers. Subsequently, when those members of the public tried to take up the matter with the sellers, they found out that the pages in question had been deleted and the sellers could not be contacted. In this connection, will the Government inform this Council:

(1) of the number of reports of online shopping fraud received by the Customs and Excise Department, the Police and other relevant government departments in the past three years, the amount of money involved and the respective numbers of relevant prosecutions and convictions;

(2) of the policies or measures in place to assist members of the public who have been defrauded in recovering the payments made to fraudsters;

(3) how the Consumer Council followed up the aforesaid type of complaints in the past three years;

(4) how the authorities follow up those online shopping fraud cases which were found upon investigation to have involved overseas criminal syndicates; whether they will take the initiative to contact the relevant departments of the countries concerned to seek assistance from them;

(5) as more and more members of the public make use of social media

platforms for online shopping, whether the authorities have studied new measures and policies to combat online shopping frauds so as to protect the consumers' rights and interests; and

(6) as it has recently been reported by the media that the credit card data of customers amassed by several online shopping platforms are available on websites associated with illegal activities (commonly known as "dark webs"), and the situation is serious, whether the authorities have received relevant reports; if so, of the details; the measures the authorities have put in place to protect the personal confidential data of members of the public from being stolen and used when they shop online?

Reply:

President,

After consulting the Security Bureau, the Constitutional and Mainland Affairs Bureau, the Office of the Government Chief Information Officer (OGCIO) and the Consumer Council, my reply to the six parts of the question is as follows:

(1) The number of complaints against unfair trade practices related to online shopping received by the Customs and Excise Department (C&ED) and the relevant enforcement statistics in the past three years are set out at Table 1. As some complainants did not provide information on the amounts involved in the complaint cases, C&ED does not have statistics on the amounts involved. The figures of online shopping fraud cases received by the Police in the past three years are set out at Table 2. The Police do not maintain prosecution and conviction figures for online shopping fraud cases (Note 1).

(2) In criminal cases (including fraud cases) handled by the Police, upon handing down judgments, the court will issue orders to direct the handling of lost properties or cash involved which were seized by the Police as exhibits during the investigation. If the court is satisfied that an exhibit belongs solely to a particular victim, it may issue an order for its return. In addition, if a bank account is found to be used for handling criminal proceeds, the Police will, where appropriate, request the bank to freeze the relevant suspicious assets. During such period, the victim may consider claiming compensation for the loss suffered through civil action. If necessary, the victim may obtain their documents relating to the case from the Police to take forward such procedures.

On the other hand, under section 36 of the Trade Descriptions Ordinance (Cap. 362) (the Ordinance), aggrieved consumers may institute civil claim for damages if they have suffered loss or damages due to conduct directed to them which constitutes a fair trading offence (Note 2). Separately, under section 18A of the Ordinance, where a person is convicted of any of the fair trading offences, the court may order the convicted person to compensate any person for the financial loss resulting from the offence.

(3) Consumers who have disputes with online traders may seek assistance from the Consumer Council. The Consumer Council acts as a conciliator in handling

disputes between consumers and traders. It assists traders and complainants to resolve their disputes, for example, by trying to contact the traders with a view to helping both parties develop mutually acceptable agreements. In cases that involve suspected illegal conduct, the Consumer Council will refer the cases to law enforcement authorities for follow-up.

(4) In handling cases of online fraud, if the Police needs to conduct investigation or adduce evidence in respect of incidents which took place outside Hong Kong, the Police will exchange intelligence and seek co-operation with relevant law enforcement agencies outside Hong Kong, and the Interpol. Besides, if local or websites outside Hong Kong are found to be conducting illegal activities, C&ED may demand such websites to remove the relevant contents or links. Depending on the need and circumstances, joint operations with enforcement agencies outside Hong Kong may also be conducted.

(5) The Police are committed to combating technology crimes (including online shopping frauds). Since 2012, the Police have put "combating technology crime" as one of the Commissioner of Police's Operational Priorities, and have been enhancing their technology, equipment and resources input in this regard. In July 2017, an enforcement action codenamed "Operation DRUMSKY" was launched to combat online shopping frauds, in which 30 persons were arrested and 162 cases and loss of about HK$890,000 were involved. In addition, C&ED attaches great importance to protecting consumer rights. C&ED will monitor different types of illegal online activities by using advanced tools for evidence collection and investigation, and initiate appropriate follow-up actions and prosecutions on complaints received.

Apart from proactive law enforcement, publicity and education are equally important in protecting consumer rights. In the study report on online shopping published by the Consumer Council in 2016, the Council reminds consumers that as online shopping becomes increasingly popular, they should be aware of some common problems associated with it. The report also gives a number of recommendations to traders, encouraging them to strictly comply with the law, adopt good business practices and enhance customer service. The "CHOICE" Magazine published by the Consumer Council has in recent years featured a good number of articles on the subject of online shopping, including giving tips to consumers on what they should pay attention to when making a purchase online by "cash on delivery" in the March 2018 issue. C&ED also reminds consumers from time to time to stay vigilant when shopping online and procure products from reputable traders. They should not trust advertisements at suspicious websites or social networking platforms easily, and should examine goods when accepting delivery to avoid incurring losses.

On the other hand, the Police's Commercial Crime Bureau established the Anti-Deception Coordination Centre in July 2017 to reinforce the combat against deception cases and raise the public's anti-deception awareness. Its major duties include monitoring and analysing the trends of deception cases, with a view to formulating and implementing combating strategies; co-ordinating anti-deception publicity work; setting up a 24-hour hotline "Anti-Scam Helpline 18222" to facilitate public enquiries and provide timely

assistance; and expediting the investigation of similar deception cases and minimising the loss of victims. The Police will regularly produce short videos and anti-crime information, as well as advise the public of the latest modus operandi of fraudsters through the Police's electronic platforms, including YouTube, the Hong Kong Police Mobile Application, the Police website, the Police Facebook page and the "Fight Scams Together" scam prevention information platform. The Police also disseminate anti-crime messages to the public through Police Magazine and traditional media (i.e. television, radio and newspapers).

(6) OGCIO attaches great importance to cyber security education and protection, and has been paying close attention to information security threat intelligence, including information circulated in the "dark web". That Office has not received any report so far regarding customer data of online shopping platforms being circulated in the "dark web". It will continue to work with the Hong Kong Computer Emergency Response Team Coordination Centre to constantly remind businesses and the public to stay vigilant, adopt suitable security measures on their computers and use Internet services safely, in order to protect personal information and guard against cyber attacks. Separately, the Office of the Privacy Commissioner for Personal Data (PCPD) has not received relevant reports either. PCPD from time to time issues or revises Codes of Practice and Guidances, such as the "Guidance for Data Users on the Collection and Use of Personal Data through the Internet" and "Protecting Privacy – Using Computers and the Internet Wisely", so as to assist data users of various trades to understand the requirements they must comply with in the online collection and use of personal data, and to remind the public to protect their personal data when using the Internet.

The Police have also been monitoring different types of alleged illegal acts on the web (including the "dark web") and will take appropriate actions in light of the circumstances. Thus far, the Police have not received relevant reports related to customer data of online shopping platforms being circulated in the "dark web". From time to time, the Police would remind the public to be vigilant when conducting online transactions, for example to patronise businesses with good reputation. Members of the public who suspect unauthorised use of their credit cards or leakage of relevant information should report to the Police as soon as practicable.

Note 1: Currently, as a general practice, prosecution and conviction statistics are only compiled in respect of offences in the law (e.g. "obtaining property by deception" or "theft") but not specific cases. Since a particular case could involve various offences in the law (e.g. online shopping fraud cases may involve "obtaining property by deception" or "dealing with property known or believed to represent proceeds of indictable offence", etc), prosecution and conviction statistics by case nature cannot be provided.

Note 2: The Ordinance prohibits specified unfair trade practices deployed by traders against consumers, including false trade descriptions, misleading omissions, aggressive commercial practices, bait advertising, bait-and-switch

and wrongly accepting payment.