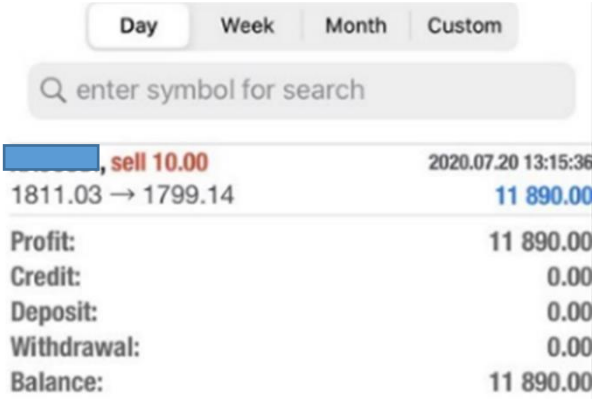
Control No.: P-1064/12-2020
Requesting country: IPSG (Financial Crimes Unit)
File No.: 2020/83543-1
Date of publication: 18 December 2020

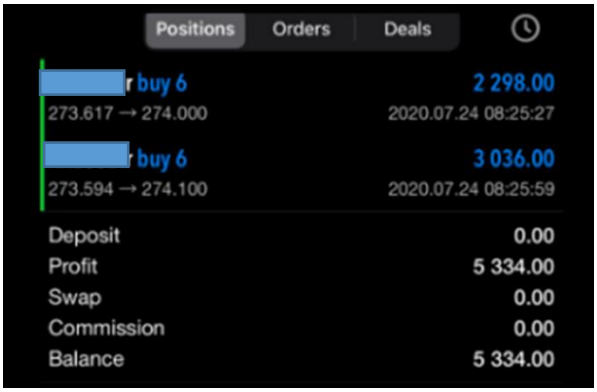
MODUS OPERANDI

INTERPOL PURPLE NOTICE

Type of offence:	Investment fraud targeting users of dating applications
Date of the offence	Ongoing
Place of offence:	Multiple countries
Country of offence:	Multiple countries
Circumstances of offence:	Since the spread of COVID-19 with increasing numbers of people socializing and dating online, criminals take advantage of the situation to lure victims on dating applications and platforms into investment fraud campaigns. These schemes are broadly categorized into three modus operandi, as follows: Artificial online romance established via dating applications are used by criminal actors to target victims for their financial engagement and investment into trading opportuntities and financial products. Victims are lured to open trading accounts and execute payments via wire transfers, card payments or cyptocurrencies and other virtual assets. Finally, the criminal actors as well as their websites become out of reach, thus causing victims to suffer full financial losses of their purported investments.
Description of modus operandi:	In recent months, IPSG (Financial Crimes Unit) has received a number of reports containing information on the same pattern and modus operandi of luring innocent victims into purported investment fraud schemes via online dating applications. Once a personal chat is established on the dating application, these criminal actors would typically propose to exchange phone numbers and continue the conversations on messenger services of different applications. It is very common for the criminal actor to claim being the same nationality as the victim, or is located in the same city or country as the victim. In some cases reported to law enforcement authorities in European countries, it was often seen that the criminal actors portrayed themselves as females with Asian origin, and used phone numbers registered in countries/jurisdictions in the Asia region (e.g. Hong Kong, Macao, etc.) to convince their targets about their genuineness. Similarly, in some other cases, the criminal actors were seen to use similar tricks to portray themselves as females with East European origin (e.g. Ukraine), targeting Russian speaking users of the online dating platforms. Once the chat and relationship has developed into what the victims perceive to be an online friendship or romance, the criminal actors start to pitch their purported success stories with trading and investment activities that led to quick and/or huge financial gains. Screenshots of the alleged trading accounts and

finanial gains of the actors are shown to the victims to generate interest and credibility. Examples of the screenshots are as follows:





In addition, victims are further lured with hot insider tips on new financial products, which would purportedly provide quick financial gains. Once the victims agree, they are directed to download a specific trading application or register a trading account on a website introduced by the criminal actors. In some cases, victims are directed by the criminal actor to contact an agent/broker, for the registration of the trading accounts. It is noted that most of these purported online trading platforms offer trading facilities in forex (foreign exchange) and virtual assets such as tokens and cryptocurrencies.

After the account is established, victims are instructed to make payment for the trading, either via telegraphic transfers to nominated bank accounts overseas, credit cards or cryptocurrencies to nominated wallet-addresses. This initial payment is purportedly required to initiate the account with the trading company. Thereafter, victims are typically lured by the criminal actor and/or agent/broker to invest more money based on the hot insider tips provided, or to reach a higher account status (e.g. Gold, VIP) to reap more returns. Victims tend to do so given the trust established with the criminal actor.

In some cases, victims received phone calls from criminal actors portraying themselves as representatives from Virtual Asset Service Providers (VASPs) and exchange services, where the victim purchased cryptocurrencies to conduct the investment. Victims were also told to make further transactions to trigger the VASP's authorization for the release of investment-profits to the victim's account.

Eventually, victims would discover that they are no longer able to access the website or log on to their trading account. The criminal actor and agent/broker also becomes completely uncontactable. Hence, the victims are not able to withdraw any investments that they have made and with little chance of ever recovering them.

Inquiries revealed that criminal actors tend to purchase used domain names that were registered several years ago. Such domain names were typically posted for sale after the initial, legitimate owners did not renew them. Criminal actors then populate their fake trading websites with fraudulent content, including claims of being licensed from financial regulators in countries such as Belize, Cyprus or Mauritius. In doing so, the company creates a false impression of being established and licensed, hence providing additional assurance to victims that the company they are investing with is legitimate.

Points of contact:	INTERPOL – Financial Crimes Unit INTERPOL General Secretariat, Command and Coordination Centre
E-mail:	INTERPOL – Financial Crimes Unit OEC-CNET-FCU@interpol.int INTERPOL General Secretariat, Command and Coordination Centre os-ccc@interpol.int (Internet) os-ccc@gs.igcs.int (I-24/7)
Telephone:	INTERPOL General Secretariat, Command and Coordination Centre + 33 4 72 44 76 76
Fax:	INTERPOL General Secretariat, Command and Coordination Centre + 33 4 72 44 71 63

Recommended precautionary action:
It is strongly recommended that you circulate this purple notice to your country's law enforcement bodies to alert them about this modus operandi and to allow them to take whatever preventive and precautionary measures they deem necessary. All recipients are strongly encouraged to share data, and provide any investigative information relating to this modus operandi.

IPSG Reference: 2020/1340/OEC/CNET/FCU/ARE