HONG KONG MONETARY AUTHORITY
香港金融管理局

Complaints Watch

Issue No. 18
13 August 2021

Complaints Watch is published by the Complaint Processing Centre (CPC) of the Hong Kong Monetary Authority (HKMA). It highlights the latest complaint trends, emerging topical issues, and areas that Authorized Institutions (AIs) may wish to place greater focus on. It forms part of the HKMA's work to promote proper standards of conduct and prudent business practices among AIs.

Complaint statistics

Jun to Jul 2021	General banking services	Conduct-related issues	Total
In progress as of 31 May 2021	530	160	690
Received during the period	479	60	539
Completed during the period	(427)	(50)	(477)
In progress as of 31 Jul 2021	582	170	752

The HKMA received 539 complaints against AIs during June and July 2021. The major types of complaints received were related to provision of banking services (91), service quality (63), remittance services (59), credit card transactions (51), lending business / decisions (47), and fund transfers (38).

What can AIs do to protect customers from investment scams?

Amidst the increasingly sophisticated attempts of fraudsters to exploit investors' thriving online activities, there has been a surge of over 100% in the number of complaints received by the HKMA in the first seven months of 2021 over a year ago whereby some bank accounts were implicated in online investment scams. Meanwhile, the HKMA has been working closely with the banking industry and stakeholders to step up capability and collaboration of the ecosystem in deterring, detecting and disrupting fraud and financial crime. This article shares our key observations from these cases as they relate to AIs' control systems as well as some good industry practices to manage financial crime risk and enhance customer protection.

In the relevant complaints, AIs were implicated mostly in "boiler room" investment scams. In these cases, victims received cold-calls, emails or mobile apps messages purportedly from overseas investment advisers or brokers, pressure-selling them different types of bogus investment. Victims were deceived to deposit funds into certain bank accounts maintained at AIs. Shortly afterwards, fraudsters remitted the funds away and disappeared[1]. Those AIs implicated in these cases became subjects of customer complaints alleging issues relating to customer due diligence and transaction monitoring for the prevention and identification of fraudsters' use of banking services for illicit purposes. It is also noted that fraudsters might have used stooge accounts to trade securities and manage fund flows in investment scams.

1 A thematic article on remittance frauds was published in the Complaints Watch (Issue No.3) on 23 January 2015. (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150123e1.pdf)

While the predicate offences (i.e. fraud) are under investigation by law enforcement agencies and/or authorities in accordance with relevant laws in Hong Kong, the HKMA requires AIs to provide responsive support to Anti-Deception Coordination Centre of the Police and fully assist in criminal investigations, including through the Fraud and Money Laundering Intelligence Taskforce (FMLIT)[2]. In addition, typologies are shared with the industry and should assist AIs to stay vigilant and incorporate alerts of emerging risks to enhance the effectiveness of control systems. It is clearly not to expect that the HKMA or AIs would be able to pre-empt all fraud and financial crime, but that when these unfortunately happen, our responses are quick, robust and targeted.

Some key observations and good industry practices for enhancing AIs' systems and consumer protection measures to combat investment scams and other financial crime are highlighted below[3].

a) Enhancement of strategies, systems of control and work planning – In the light of emerging risks, AIs have proactively enhanced their relevant business strategies, systems of control and work plans to incorporate the features of investment scams and other risk indicators received from various sources, including media reports, complaints received, as well as intelligence and risk alerts shared through FMLIT or regulatory authorities. For example, noting that fraudsters may operate investment scams by organising deceptive discussions and using a number of stooge accounts to trade securities and manage fund flows, AIs have incorporated the relevant risk indicators in their anti-money laundering

2 FMLIT is a public-private partnership established in 2017, led by the Hong Kong Police Force with participation by the HKMA and a number of retail banks. Similar to arrangements in other international financial centres, FMLIT targets current and emerging financial crime threats through information sharing, both at the strategic and tactical level. FMLIT has been recognised internationally in a report published by the Royal United Services Institute, a renowned think tank, in 2020.

3 For more details, please refer to the HKMA's circular letter dated 26 April 2021. (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1.pdf)

systems to facilitate identification and reporting of suspicious accounts and transactions to the Joint Financial Intelligence Unit for appropriate follow-up.

b) Information sharing – Many AIs have deployed resources to do Internet searches with a view to detecting suspicious signs of investment scams involving the abuse of bank accounts. There is also increasing use of advance technologies such as artificial intelligence in recent years to facilitate data analytics and detection of stooge account network and suspicious fund flows[4]. On a sectoral basis, FMLIT has provided an important information sharing platform for disrupting money laundering and financial crime including investment scams, assisting to curb displacement of risk across the system. Since its establishment in 2017, FMLIT has successfully identified over 11,000 bank accounts previously unknown to law enforcement agencies, leading to restraint or confiscation of about HK$700 million of crime proceeds involving financial impacts on customers and/or AIs themselves.

c) Consumer education and alerts – Many AIs have made efforts on consumer education and alerts against fraud and financial crime. For example, prominent alerts are posted at their branches and websites to promote public awareness of deception devices and preventive knowledge. Educational messages and smart tips are updated continuously to address emerging types of fraud and financial crime including investment scams. Some AIs have set up online information centres or thematic webpages for this purpose, with hyperlinks to the relevant webpages of financial regulators, law enforcement agencies and industry

4 Please refer to the HKMA's report titled "AML/CFT Regtech: Case Studies and Insights", published on 21 January 2021. (https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf)

associations.

It is important that AIs deploy sufficient resources for proper handling of complaints in this area, and work closely with other stakeholders in the ecosystem to enhance effectiveness of collaborative efforts to deter and detect possible abuse of the banking system for illicit fund flows, and to disrupt investment scams and crime incurring financial losses to customers and/or AIs. As part of the preventive measures, sufficient staff training should be provided while consumer education should be sustained and updated as new threats of stooge account networks emerge. In this connection, apart from ongoing consumer education for staying alert to investment and phishing scams, the HKMA has issued a **Facebook post** today reminding bank consumers to say "NO" to any requests or financial rewards for selling or lending one's bank account to a third party which may constitute a money laundering offence (「切勿貪心搵快錢，戶口借人洗黑錢」)[5]. AIs are strongly encouraged to reinforce the educational messages in their ongoing communication with customers and potential customers.

Comments and feedback on *Complaints Watch* are welcome. Please email them to *bankcomplaints@hkma.gov.hk*.

5 The following posts are also available at the HKMA's Facebook account.

- 智破疫情網絡陷阱 (9 June 2020)
- 又想呃密碼 (7 July 2020)
- Fact Check 資料來源 (24 July 2020)
- 一次性密碼 先對啱後輸入 (23 June 2021)
- 數碼 Key 睇緊啲 撳 Link 前要三思 (5 July 2021)