Link to Article on website

Fighting cyber-fraud in Hong Kong - what can we do?

There has been a phenomenal increase in the number of reported cyber related crimes and suspicious transactions reported in Hong Kong in recent years, inevitably resulting in huge financial losses suffered.

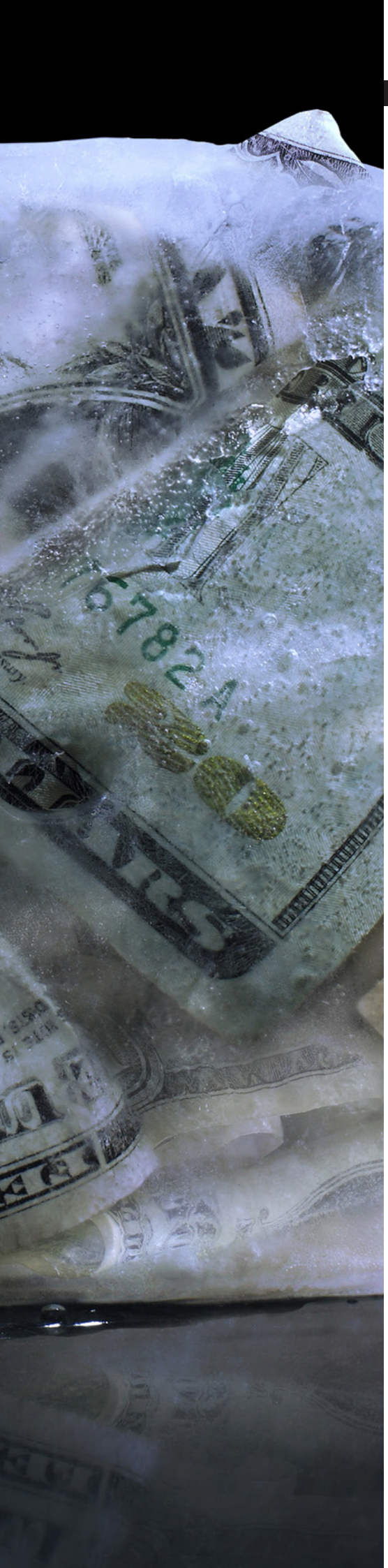
BY:
Richard Keady, Partner
Aline Mooney, Associate
BIRD & BIRD LLP

AS ONE OF THE WORLD'S LEADING FINANCIAL CENTRES, IT IS UNSURPRISING THAT HONG KONG is facing a rapidly growing threat of cyber fraud, money laundering and terrorist financing. There has been a phenomenal increase in the number of reported cyber related crimes and suspicious transactions reported in Hong Kong in recent years, inevitably resulting in huge financial losses suffered. Victims are often left with little or no remedy given that cyber-crime and in particular email scams, are by far the hardest crimes to detect and the toughest to beat given the increasingly sophisticated scams used by fraudsters.

International fraud networks are continuing to scam business individuals and companies worldwide - most scammers are based overseas and the funds are hard to retrieve when the fraud is detected because it is often quickly siphoned off into different accounts and moved around the world.

Fighting dirty money

Hong Kong's current anti-money laundering regime has come under attack in recent years given the surge in sophisticated cyber-attacks linked to



local, national and international criminal syndicates. Given its strong links with Mainland China in terms of finance, trade and transport, Hong Kong is naturally exposed to the threats of cyber-fraud and money laundering. Regulators are therefore coming under increasing pressure to respond to these risks and implement more robust anti-money laundering polices.

The Financial Action Task Force (FATF), an inter-governmental body which oversees measures for combating money laundering and terrorist financing looks set to put further pressure on Hong Kong's financial institutions and regulators to intensify their efforts against the risk of cyber-fraud and to enhance measures to detect and prevent financial crime and money laundering threats. The concern remains that cyber-crime will continue to rise and international businesses may start to blacklist Hong Kong in favour of what are seen as more 'secure' financial global hubs with more stringent regulatory and legal frameworks.

The rise of the 'email scam'

In Hong Kong in particular, one of the most common cyber-attacks is the impersonation (by email) of business partners or senior financial staff in a company. Financial institutions are routinely coming across this type of problem. A typical example is when a fraudster hacks a company's email server and requests payments to be made to various bank accounts. The email is seemingly sent from a 'genuine' contact so the company mistakenly takes this request at face value and remits the funds as instructed. Typically the funds are long gone by the time the company realises the mistake and unsurprisingly, identifying the fraudster is incredibly difficult if not impossible.

To have any chance at recovering the stolen funds, victims (or their representing law firms) must act fast. Once the fraud has been spotted (or even suspected), companies must immediately notify both the remitting and receiving banks and request that they freeze the accounts. The next step is notifying both local police and the Hong Kong police. If the Hong Kong police are satisfied that a fraud has occurred, they will issue a 'no consent letter' to the bank holding the funds. This essentially puts a temporary freeze on the bank account so to the extent there are any funds left in the account, they will be frozen.

The police will then often advise the victim to seek a mareva injunction in the Hong Kong courts which is a form of interlocutory relief to formally freeze the assets while the substantive action against the fraudster is heard and decided by the court. A garnishee order may also be utilised if default judgment has been obtained against the defendant (which it typically will be as a fraudster will not contest the claim and alert the police to his or her whereabouts). Once a garnishee order is obtained and served, the recipient bank would then be required to release any funds held in the fraudster's bank account.

Pave the way for greater ease of preventing proceeds of crime from being moved so quickly (rather than of being moved)

Notwithstanding the above, it is often difficult to obtain successful enforcement actions against the perpetrators of cyber-fraud as they can so easily stay anonymous in cyberspace. However, a recent judgment of English Commercial Court (CMOC v Persons Unknown [2017] EWHC 3599 (Comm)

has provided some interesting and helpful guidance for this type of situation which could pave the way for greater ease of preventing proceeds of crime of being moved so quickly.

In this case, alleged frauds were committed by unknown persons who infiltrated the email account of one of the senior managers of the targeted company. The fraudsters were then able to send payment instructions to the company's financial administrators to remit a number of very large payments from the company's bank account, at Bank of China in London, to various other banks around the world. The sums fraudulently transferred were in the region of £6.3 million in total.

In the first of its kind, the court granted a worldwide freezing order (WFO) against the assets of 'persons unknown' who perpetrated the fraud but remain unidentified. The court also noted that a WFO can be used to further other ancillary relief against third parties e.g. the recipient banks of the fraud to assist in tracing and recovering the stolen funds which would not be available unless a freezing order was in place.

Although courts in Hong Kong currently have the power to grant an injunction against unnamed defendants, the courts must be satisfied that the description as to the unknown defendants' conducts is sufficiently certain such that only those who should necessarily be included can be identified. The decision of the English courts will therefore be of significance to the Hong Kong courts as English authorities are regarded as persuasive authority in the Hong Kong courts.

The Future

In light of the above, it's clear that financial institutions in Hong Kong need to recognise the damage that cyber-crime is having across all sectors and in the context of its international business with overseas investors and businesses. Banks in particular need to pay more attention to what policies they can implement to ensure that the impact of money laundering in Hong Kong is eradicated or significantly reduced. New technologies such as AI and biometric security mechanisms are making financial services more convenient but sometimes act as a double edged sword - with savvy fraudsters always seemingly one step ahead.

However, biometric technology has become increasingly accessible and reliable, and has become more appealing to banks, financial institutions and regulators in their bid to reduce fraud and cyber-crime. Equally, artificial intelligence and data analysis that can detect abnormal transactions more easily, and understanding the related risks associated with this type of technology may serve to provide at least the minimum security measures required to keep money launderers and cyber-fraudsters at bay.

In terms of protecting companies from the consequences of email scams, the Hong Kong courts appear to be sympathetic to victims to cyber-fraud and this trend is likely to continue given the vast amount of cyber-crime cases that are ending up in the Hong Kong courts both from local and overseas companies.

Although ongoing, the CMOK case is still welcome news for the international business and finance world, allowing victims of cyber-fraud to pursue anonymous fraudsters in a bid to recover losses as a result of criminal activity. ■