DORSEY
DORSEY + WHITNEY LLP

Hong Kong and Overseas Businesses Defrauded of over HK$1.8 billion (US$231m) in 2016

by Steven C. Nelson

Email wire fraud scammers continue to target local and international businesses with victims suffering millions of dollars of lost funds wired to Hong Kong bank accounts.

In December 2016, the Hong Kong Legislative Council Panel on Security published a Paper ("**Paper**")[1] reporting that technology crime cases received by the Hong Kong Police Force (including business email compromise scams) have already defrauded local and international businesses of over HK$1.8 billion (US$231m) this year.

A report by the *South China Morning Post* reported one instance whereby an employee of a bank in Europe was deceived into transferring about HK$500m (US$64m). The email scammer used a ploy commonly used by email scammers to defraud the unsuspecting business by impersonating a senior executive by email and providing wire transfer details and payment requests to Hong Kong bank accounts.[2]

In Hong Kong, the annual number of local reports of technology crimes has increased significantly by 24 times from 272 cases in 2002 to 6,862 in 2015. As at September 2016, the number of cases has already hit 4,537. Over the past six years, the respective annual financial losses have also increased by 30 times from HK$60 million (US$7.7m) in 2010 to HK$1.8 billion (US$231m) in 2015. In 2016 (as at September), the loss is around HK$1.87 billion (US$240m).[3]

Typically, once any money and has been wire transferred from an overseas bank account to a Hong Kong bank account as a result of fraud, the money is quickly transferred again to another account out of Hong Kong making recovery much more difficult.

The potential losses can be significant, and the scams are becoming highly sophisticated, including the apparent covert surveillance of emails within a business, to enable the scammers to impersonate high level executives to execute or arrange large sum wire transfers to Hong Kong bank accounts.

Related People

- Steven C. Nelson

Related Capabilities

- International Arbitration & Litigation
- Financial Services Regulatory
- Privacy & Social Media
- Anti-Corruption
- Asia-Pacific
- China

The publication of this Paper is a timely reminder of the need for international businesses to implement safeguards to protect against business email scams and other fraud and to act expeditiously to take remedial action in the event of discovering any fraud.

For a detailed review of business email scams and further information, please see our *Guide to Protecting Against Email Wire Fraud Scams and Recovering Funds Wired to Hong Kong* here.

[1] Measures to combat technology crimes and proposed creation of a permanent Chief Superintendent of Police post of the Cyber Security and Technology Crime Bureau: LC Paper No. CB(2)282/16-17(05)

[2] http://www.scmp.com/news/hong-kong/law-crime/article/2053703/international-email-scams-involving-hong-kong-hit-hk15

[3] See paragraph 4 of the Paper.