LHAG Insights

Corporate & Commercial Disputes
| Technology, Media and Telecommunications

ABOUT THE AUTHORS

G. Vijay Kumar
Partner
Corporate & Commercial Disputes | Technology, Media & Telecommunications
E: vkg@lh-ag.com

Brandon Loo Yung Wen
Associate
Corporate & Commercial Disputes | Technology, Media & Telecommunications
E: bly@lh-ag.com

18 OCTOBER 2022

Rampant Online Scams: What are the authorities doing to address the problem?

Introduction

As of late, online fraudulent activities, or more commonly known as "online scams", has become an increasingly frequent occurrence worldwide. In Malaysia, these online fraudulent activities come under the purview of the Malaysian Communications and Multimedia Commission ("**MCMC**"), a statutory body empowered by the *Malaysian Communications and Multimedia Commission Act 1998* ("**CMCA**") which governs the nation's communications and multimedia sector. On 13.6.2022, MCMC reported that there were an alarming number of 1,290 cases of fraudulent transactions between the months of January 2021 to May 2022. This number excludes cases that have gone unreported by members of the public. Given the globally increasing number of online fraudulent cases at an alarming rate, we take a look at the steps that are being taken by the authorities in Malaysia and other countries in response to the problem.

United Kingdom

In the U.K., the Government has begun drafting the *Online Safety Bill*. Recent changes to the Bill include the imposition of a legal duty on social media and search engines to prevent paid-for fraudulent advertisements from appearing on their platforms. These will cover unlicensed financial promotions, fraudsters impersonating legitimate businesses, as well as advertisements by fake companies.

The change will undoubtedly affect the largest and most influential social media platforms and search engines. According to the Bill, such platforms and search engines will need to put in place "*proportionate systems and processes to prevent the publication and/or hosting of fraudulent advertising on their service and remove it when they are made aware of it*".

This could mean that providers must implement systems to properly vet advertisers and advertisement contents before publishing on their platform.

European Union

On 5.7.2022, the European Parliament approved the final version of the *Digital Services Act* ("**DSA**").

The DSA is a landmark piece of legislation which updates the *E-Commerce Directive of 2000*.[1] It aims to protect online consumers and their fundamental rights by generating a safer digital space and by creating an open and transparent online environment. It imposes a new set of due-diligence requirements on businesses. This comprises of newly introduced rules related to, inter alia, illegal content, algorithm oversight, content moderation, compulsory information to be furnished to both businesses and consumers, along with actions against those who violate companies' terms of service.

The primary concern of the DSA are digital services which include, search engines, online marketplaces, social media and content-sharing platforms, travel and accommodation platforms, cloud and web-hosting service providers, app stores, as well as Internet Service Providers and domain name registrars and registries.[2]

This Act will be applicable across the E.U. fifteen months from the date of publication in the E.U. Official Journal or on 1 January 2024, whichever comes later.[3]

United States

In the U.S., the *Computer Fraud and Abuse Act* was passed in 1986. Since then, many types of online fraud cases were prosecuted under provisions of this Act.

---

[1]Morar, 'The Digital Services Act's lesson for U.S. policymakers: Co-regulatory mechanisms' (Techtank, 23 August 2022) <https://www.brookings.edu/blog/techtank/2022/08/23/the-digital-services-acts-lesson-for-u-s-policymakers-co-regulatory-mechanisms/>

[2]Werneck, 'EU:What New Digital Services Act (DSA) And How Does It Affect Your Business?' (mondaq, 7 September 2022) <https://www.mondaq.com/social-media/1228154/what-new-digital-services-act-dsa-and-how-does-it-affect-your-business>

[3] European Commission, 'The Digital Services Act package' <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

There are also several laws which deal with various types of online scams. For instance, under the Federal Law of the U.S., the 18 U.S. Code Section 1343 covers cyber fraud or fraud perpetrated by e-mail or the Internet.[4] It also carries a harsh punishment of up to twenty years in federal prison. Meanwhile, the 18 U.S. Code Section 2028 prohibits fraud in connection with identification documents, authentication features and information.

Apart from this, some years ago, the U.S. government had launched an international database to protect consumers from online fraud.[5] This is run by the Federal Trade Commission and it gathers confidential fraud information from law enforcement officials across the globe.

Finally, an updated listing of common scams and frauds in the US is available on the U.S. government website to alert the public.[6]

Singapore

As for Singapore, there is currently no legislation which specifically tackles online-related scams or online fraudulent activities. However, it has been reported that the Singapore legislature is looking into methods of tackling online scams, as the issue was brought up earlier this year during a parliamentary session.

In the meantime, the Singaporean authorities are also looking to address this issue through a variety of other measures.

Singapore SMS SenderID protection registry

On 4.3.22, the Infocomm Media Development Authority ("**IMDA**") has set up a Singapore SMS SenderID protection registry to allow organisations to protect their customers from Spoofed SMS sender IDs.[7] IMDA has been collaborating with the Singapore Police Force, Government agencies and private sector partners. Under the proposal, a transition phase would commence in October. Thereafter, registration would be mandatory starting from this year-end.

---

[4] Greg Hill & Associates, 'What Is Internet Fraud? The Defenses? The Punishment?' <https://www.greghillassociates.com/what-is-internet-fraud-the-defenses-the punishment.html#:~:text=Under%20federal%20law%2C%20the%20controlling,twenty%20years%20in%20federal%20prison>

[5] Left, 'US moves to tackle online fraud' (Guardian, 25 April 2001) <https://www.theguardian.com/technology/2001/apr/25/internetcrime.internet>

[6] USAgov, 'Scams and Frauds' <https://www.usa.gov/scams-and-frauds>

[7] SGNIC, 'SMS Registry' <https://www.sgnic.sg/SMSRegistryeinvoicing/smsregistry>

Sender IDs permit the identification of the sender of an SMS message in such a way that a word or phrase appears rather than a number. As such, organisations have the option to block scam messages from being sent by scammers who are using a registered sender ID. This prohibits scammers from impersonating banks and other organisations.

In order to make the public vigilant to potential scam calls, the IMDA has also incorporated other measures such as by blocking numbers that are regularly spoofed and prefixing incoming international calls with the "+" sign.

ScamShield app

The ScamShield app was jointly developed by the National Crime Prevention Council and the Open Government Products team, a unit within the Government Technology Agency. The app has adopted artificial intelligence to filter scam messages and can also block calls from numbers reported by users, or those on a list managed by the Singapore Police Force. The app is designed to learn words often used in fraudulent texts, including "*gambling*", "*repayments*" and "*loans*" and subsequently determines how these words are used in conjunction with each other. This diminishes the possibility of users being contacted by scammers.[8]

Anti-Scam Command

The Anti-Scam Command ("**ASCom**") was operationalised on 22.3.22 to achieve greater synergy between various scam-fighting units within the Singapore Police Force, by integrating scam investigation, incident response, intervention, enforcement, and sense-making capabilities under a single umbrella. The ASCom comprises the Anti-Scam Centre, three Anti-Scam Investigation Branches, and oversees the Scam Strike Teams situated within each of the seven Police Land Divisions. It partners with more than 70 financial institutions, online marketplaces, and telecommunication service providers. Through the joining forces of these parties in real-time, ASCom targets to promptly freeze bank accounts which are suspected to be involved in scammers' operations.

As many scams are initiated from overseas locations, the ASCom works closely with foreign law enforcement counterparts to detect and tackle emerging crime trends.[9]

---

[8]Chia, Leck, Lim, Magnus, Seetoh and Toh, 'Singapore: Authorities introduce measures to combat SMS- Phishing scams' (Baker Mckenzie, 19 February 2022) <https://www.globalcompliancenews.com/2022/02/19/singapore-authorities-introduce-measures-to-combat-sms-phishing-scams280122/>

[9] Singapore Police Force, 'Opening of Anti-Scam Command Office' (Police.gov.sg, 6 September 2022) <https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office>

LH AG ADVOCATES AND SOLICITORS

Malaysia

In Malaysia, the *Communications and Multimedia Act 1998* ("**CMA 1998**") does not currently have any provision to hold social media or search engine service providers responsible for online scams. There also does not appear to be any initiative by the Government to update the *CMA 1998* in this regard. There are however several laws in place to prosecute perpetrators of online scams. For instance, Section 16 of the *Consumer Protection Act 1999* makes it an offence for any person demanding or accepting payment without intending to supply. Furthermore, Section 18 of the *Trade Descriptions Act 2011* provides for false or misleading statement in advertisement.

It has been reported that the regulator, MCMC, is taking steps to tackle the problem by collaborating with ISPs and Telcos in organising a scam prevention campaign which aims to create awareness amongst the public.

There is also a CCID Scam Response Centre in place which is managed by the police's Commercial Crime Investigation Department. This is a one-stop centre supported by MCMC, Payments Network Malaysia (**PayNet**), Bank Negara Malaysia and other financial institutions in response to scam incidents. It functions as the first recipient of information on fraudulent incidents from victims and allows the public to receive verification in regard to suspicious calls and messages.

The Malaysian police force is also playing their part in creating public awareness. The police force recently recruited 104 key opinion leaders ("**KOLs**") as ambassadors for its anti-scam campaign.[10] The KOLs consist of celebrities, influencers, sports icons, business, and religious scholars. The idea utilises the KOLs, who has the reach to efficiently and effectively spread awareness about the tactics of scammers to the public.

Conclusion

As highlighted above, whilst there is legislation in place in Malaysia to penalise the offenders, it is clear that more needs to be done to safeguard the public from falling prey to online scams. In this regard, a more proactive and targeted approach by the Government is of critical importance. The awareness campaigns are a step in the right direction. However, it is suggested that the Government should also consider adopting other measures undertaken by other countries, some of which are highlighted above to curb the rampant increase of online scams.

[10] Zolkepli, 'Celebs and influencers recruited for anti-scam drive' (TheStar, 14 September 2022) <https://www.thestar.com.my/news/nation/2022/09/14/celebs-and-influencers-recruited-for-anti-scam-drive>

Brandon Loo Yung Wen (Associate) and **Chan Wei Li** (Pupil-in-Chambers)

If you have any queries, please contact associate**, Brandon Loo Yung Wen** (bly@lh-ag.com) or his team partner **G. Vijay Kumar** (vkg@lh-ag.com).

Head Office
Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office
Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office
51-13-E Menara BHL
Jln Sultan Ahmad Shah
10050 Georgetown
Pulau Pinang
Tel: +604 299 9668
Fax: +604 299 9628

Email
enquiry@lh-ag.com

Website
www.lh-ag.com

Published by the Corporate & Commercial Disputes | TMT Practice