Asian Journal of Law and Governance
e-ISSN: 2710-5849 | Vol. 6, No. 3, 11-21, 2024
http://myjms.mohe.gov.my/index.php/ajlg

The Consumer Protection Framework of Macau Scam in Malaysia

Afida Mastura Muhammad Arif[1*], Aqilah Hairul Anuar[1], Elistina Abu Bakar[1], Sharifah Azizah Haron[1], Syuhaily Osman[1], Zuroni Md Jusoh[1]

[1] Department of Resource Department and Consumer Studies, Faculty of Human Ecology, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

*Corresponding Author: afidamastura@upm.edu.my

Received: 25 July 2024 | Accepted: 3 September 2024 | Published: 30 September 2024

DOI: https://doi.org/10.55057/ajlg.2024.6.3.2

Abstract: *Technological advancements have enabled the rise of various fraudulent schemes, with the Macau or phone scam becoming particularly prevalent in Malaysia. Regardless of the extensive publicity surrounding the Macau scam, every individual is susceptible to becoming a victim. Macau scam poses a significant threat, causing victims to lose their hard-earned money and suffer severe financial and psychological consequences. Hence, the primary aim of this study is to explore the consumer protection framework that safeguards consumers from Macau scammers. The investigation encompassed the current legislation and institutions pertaining to the Macau scam, which includes the existing laws and institutions related to the Macau scam. Document analysis was employed to collect information from government reports, journals, articles, laws, and other relevant materials concerning scams. The research findings suggest that the current consumer protection framework regarding the Macau scam in Malaysia can be further enhanced. Such improvement can be accomplished by strengthening the current legislation and advocating for measures to educate consumers.*

Keywords: Artificial Intelligence, Macau Scam, Institutional Framework, Legal Framework, Consumer Education

---

1. Introduction

The digital economy, comprising online transactions, e-commerce, digital banking, and mobile financial services, has yielded numerous advantages and prospects. Such activities have profoundly changed the world and have impacted human life tremendously. Digital transformation is, however, challenging and has a huge impact, especially on the security aspect. It has also spawned new obstacles, such as a heightened susceptibility to scams and fraud. Scammers have discovered methods to take advantage of the digital environment and focus on individuals, businesses, and the worldwide economy. The advancement of technology has also led to the emergence of a plethora of new scams, both in Malaysia and worldwide. Scams refer to fraudulent activities that exploit mass communication technology to deceive individuals and obtain their money (Whitty, 2020). Scammers can easily connect with unsuspecting individuals and commit fraud using various techniques. Consumers are, therefore, more vulnerable to a wide range of scams.

Among the commonly reported scams in Malaysia are Macau scams, love scams, online shopping scams, and investment scams (Nur Hanani, 2020; Bernama, 2020). Other scams include work-from-home, phishing, identity theft, and inheritance scams (Adib & Arfa, 2020; Yeoh, 2020; Nurul Hidayah, 2020). Among these scams, there seems to be a rise in the number of victims of the Macau scam, named after the Macau Chinese Special Administrative Region, where the practice is reputed to have originated. The Macau scam is also known as a phone or telecommunication scam since it is a fraud committed over the phone. A total of 16,752 reports involving a loss of 40 million related to scam calls have been received by the National Scam Response Centre since its establishment in October 2022 (Harun et al., 2023). According to Truecaller, a mobile app that helps block unwanted calls, 63% of spam calls in Malaysia are categorized as fraudulent (Tan, 2023). Phone calls (56%) and WhatsApp applications (54%) were identified as the top two platforms used by scammers to target victims (Tan, 2023).

Phone scams are unfortunately widespread in Asia. Scammers in Thailand primarily use phone calls (88%) and SMS (59%) as their preferred methods of communication (Bangkok Post, 2023). Phishing text messages, calls related to loan scams, cost-on-delivery, e-commerce scams, impersonation of government officials, and fake part-time job announcements are all examples of the types of fraudulent activities that fall under the umbrella of phone scams in Thailand (The Nation, 2023). On the other hand, among the well-known frauds in Indonesia are the "one ring scam," also known as the "Wangiri scam," and fake hospital/injury calls in which a caller claims to have a friend or family member in the hospital and asks for money to be sent for treatment (The Jakarta Post, 2019).

The Macau or phone scams are indeed a global phenomenon that affects consumers worldwide. Scams are a problem in developed nations as well. Phone scams are a major concern in Singapore, with scammers using a variety of tactics to deceive and defraud unsuspecting individuals. Among the types of phone scams in Singapore are government impersonation, fake friend calls as well as job scams (Tang, 2024). In the United Kingdom, thousands of people are being targeted every day. The types of phone scams include impersonation scams (government agencies such as HM Revenue and Customs (HMRC)), job scams, technology support scams and cost of living scams (posed as energy representatives or offering fake government support schemes) (Which, 2024). In Australia, phone scams are a common method used by scammers to deceive the public. These scams often involve scammers pretending to be from well-known organizations, such as government agencies, law enforcement, banks, telecommunication providers, investment firms, and law firms (Scamwatch, n.d.). In 2021, Australians reported a record AUD$211 million in losses due to scams, with phone-based scams accounting for over AUD$63.6 million of the losses (ACCC, 2021).

Despite widespread coverage in newspapers, news websites, and social media, people still fall for scams despite. The alarming and growing trend in Macau scams poses a genuine concern and risk to consumers. It also posed a significant danger, as it entails the financial losses of victims' hard-earned money. As for the victims, the financial losses caused significant impacts on them, given that the victims often suffer severe financial and psychological impacts (Conway, 2021).

2. Artificial Intelligence and the Opportunities of Macau Scam

Scammers leverage artificial intelligence (AI) technology to augment their tactics, rendering their scams more focused and perilous. AI is utilised in phone scams in various ways. Firstly, voice cloning was made possible by AI technology. Voice cloning is a technique that enables scammers to assume the identities of prominent figures, elected officials, and even close friends and relatives (Mohd Reda, 2024). Secondly, the utilisation of AI-driven voice cloning technology enables scammers to imitate the vocal patterns of trustworthy individuals, such as bank officers (Williams, 2023). Impersonation empowers them to mislead individuals into believing an urgent situation or problem that demands immediate attention.

Thirdly, phone scams that utilise AI often employ spoofing techniques, which complicate the process of identifying the source of the calls (Commission for Communications Regulation, 2023). Scammers have the ability to employ artificial intelligence (AI) to imitate authentic phone numbers or voices, which poses difficulties in recognising and tracing their whereabouts. Next, scammers can automate their phone calls with the assistance of AI tools, thereby expanding their reach to a greater number of prospective victims (Commission for Communications Regulation, 2023). They can increase the efficacy of their scams by automating the calling process and generating text messages using AI. Finally, by utilising AI, scammers are able to deliver more targeted and impactful phone calls. Through the collection of information about their potential victims from a wide variety of sources, they are able to personalise the scams that they perpetrate. Because of this, scammers are able to be more convincing in their respective schemes.

3. Factors Explaining Why Victims Fall for Phone Scams

Victimology and psychology research has been applied to various behavioural issues, including provocation, responses to violence, and criminal victimisation (Wan Sulaiman et al., 2022). Models based on victimology, psychology, or a combination of both offer explanations for the processes and pathways that lead to victimisation behaviours (Gainsbury, 2019; Mouton et al., 2016; Norris & Brookes, 2021; Williams et al., 2017). The existing literature offers evidence that certain behaviours (such as impulsivity, negligence, gullibility, irresponsibility, and excessive trust), specific emotions (such as greed, desire, loneliness, and attachment), and specific cognitions (such as failure to recognise deception cues, reliance on heuristics, and low need for cognition) are more prevalent among individuals who fall victim to scams, despite being aware of the existence and prevalence of such scam activities (Wan Sulaiman et al., 2022). In many cases, victims underestimate their vulnerability to scams (Williams et al., 2017). Hence, victims frequently do not recognise their vulnerability or susceptibility until they are victimised. The inability to identify fraudulent communications may be a contributing factor to the victimisation experience (Norris & Brookes, 2021).

Raising awareness about the prevalence of certain crimes is a strategy to mitigate an individual's future crime risk (Bidgoli & Grossklags, 2017). However, contrary to what has often been assumed, the victims are actually aware of the danger of falling victim to a scam (Farahanim & Tengku Elena, 2023). All participants in the latter's study were aware of the scams operating in the country. Nevertheless, the participants fell victim to scams due to the factors of trust and panic. According to Lu et al. (2020), a significant factor contributing to individuals becoming victims of scams is their firm trust in the scammers. The trick was to present a convincing self-introduction that sounded so professional that it convinced the victims that the calls were legitimate (Farahanim & Tengku Elena, 2023). This tactic is effective because victims tend to trust and fear law enforcement authorities such as the police, the Inland Revenue Department, court officials and the Customs Department (Parkaran, 2022).

Scammers pose as police officers who, when speaking on the phone, seem very authoritative and capable of frightening and panicking their victims (Muhammad Basir, 2020). Moreover, the scammers induce a state of panic by employing threats, warnings, and dares to ensure that the victims succumb to their trap (Shaari et al., 2019). For example, a scammer posing as a

Asian Journal of Law and Governance
e-ISSN: 2710-5849 | Vol. 6, No. 3, 11-21, 2024
http://myjms.mohe.gov.my/index.php/ajlg

bank officer contacts the victims and notifies them about an outstanding charge on their credit cards (Farahanim & Tengku Elena, 2023). Hence, scammers employ high-pressure techniques to create a sense of urgency, fear or excitement to manipulate victims into making quick decisions. The syndicates also employ professional trainers who constantly improve their strategies, making it challenging for law enforcement agencies to detect and expose their illicit activities. They are always a step ahead of the law enforcement agencies. (Goh, 2019).

4. Legal Framework

Consumer protection encompasses measures aimed at preventing malpractice and exploitative practices that harm consumers. The Malaysian National Consumer Policy (NCP) has put great consideration on three aspects of consumer protection: self-protection, self-regulation, and legal protection. Nevertheless, the policy was last reviewed in 2010. Since then, lots of development has taken place worldwide in increasing consumer self-protection, business self-regulation and the relevant laws on scams. For example, the United Nations Guidelines for Consumer Protection (UNCGP), being the basis for NCP, was reviewed and adopted by member states in 2015 (UNCTD, 2018). Moreover, the latest European Union (EU) consumer policy, the New Consumer Agenda 2020-2025, sought to strengthen consumer protection throughout the EU, addressing consumers' immediate needs during the COVID-19 pandemic and increasing their resilience (European Commission, 2020). In 2020, the OECD released a Policy Guidance Note to help policymakers and oversight authorities implement the G20/OECD High-Level Principles on Financial Consumer Protection in digital environments and protect consumer assets from fraud and misuse and data and privacy (OECD, 2020).

The Consumer Protection Framework mainly consisted of two major parts: protection through policy, laws and regulation, as well as self-protection propagated through consumer education. The legal framework refers to the legal provisions that are applicable to the Macau scam. The word “Macau scam” is not mentioned under the law. A scam is, however, defined in *Pendakwa Raya* v *Ihebom Obinna Edward* [2017] MLJU 2263 as “a fraudulent scheme performed by a dishonest individual, group, or company in an attempt to obtain money or something else of value”. Nevertheless, the Penal Code adopts the term "cheating," which is synonymous with "fraud." (Nasaruddin & Zulkefly, n.d.). Cheating under section 415 of the Penal Code means *deceiving, fraudulently or dishonestly inducing another person to deliver any property to any person or to consent that any person shall retain any property*. According to Section 417 of the Penal Code, anyone who cheats faces imprisonment for a term of up to five years, a fine, or both. A more detailed section of the Penal Code that addresses cheating and dishonestly inducing the delivery of property is section 420. Any person who is found to have violated this section is subject to a fine, whipping, and imprisonment for a term not less than one year and not more than ten years. In addition, section 170 of the Penal Code provides the punishment for personating a public servant.

The Macau scam is a serious threat to the nation as it is an organised crime syndicate involving masterminds such as unscrupulous law enforcement agencies and corrupt police officers as well mule account holders (Akhbar, 2020, Siti Farhana, 2021). Scam networks in Macau "rent" or create mule bank accounts from unwitting holders and use them to transfer victims' funds to themselves. Even if a mule account holder is not directly involved in whatever their "renter" does, they can still be charged under section 424 for concealing funds, which carries a sentence of imprisonment up to five years, a fine, or both upon conviction. The consequences of having a mule account are severe, as the account holder will have a criminal record, and the bank will close their accounts (Hasjun, 2021). Furthermore, this syndicate group, which was also linked to international networks, made it difficult for eradication actions to be implemented comprehensively (Jabatan Siasatan Jenayah Komersil, 2022). Local and international lines, primarily from Hong Kong, are used by perpetrators to dupe victims into handing over large sums of money (Siti Farhana, 2020).

The Macau scam is also related to money laundering. In the recent crackdown on a Macau syndicate in 2021, two directors of a company involved in a Macau scam syndicate were charged for receiving RM2.1 million in proceeds from illegal activities from two Chinese nationals under the money laundering law (Rahmat, 2021). Macau scam is not simply a scam between a scammer and a victim, but this unethical activity involves a wide range of accomplices, and the implication is far-fetched. Illegal deposit-taking can be charged under section 137(1) of the Financial Services Act 2013 (FSA), while the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) require reporting institutions to disclose suspicious financial activity. The regulators that enforce these laws are the Royal Police of Malaysia, Bank Negara Malaysia, and the Malaysian Anti-Corruption Commission. Since the Macau Scam syndicate is a symptom of a larger problem involving a diverse group of people, eradicating the scam involves agencies of different jurisdictions. However, the involvement of several agencies regulating Macau scam laws may have resulted in different applications, different rules and different enforcement.

It is important to note that these regulations and initiatives are aimed at addressing the challenges posed by AI-enabled phone scams. However, scammers are constantly evolving their tactics to exploit AI technology, and consumer vigilance remains crucial in identifying and avoiding fraudulent activities. This makes it challenging for regulators to keep up with the latest tactics and develop effective enforcement strategies. Furthermore, the issue of identification and tracking of consumers whereby AI-enabled phone scams often involve spoofing techniques that make it difficult to trace the origin of the calls. In addition, phone scams can originate from different countries, making it challenging to enforce regulations across borders. Enforcing regulation on AI-enabled phone scams requires significant resources including skilled personnel, advanced technology and international collaboration. Thus, many regulatory bodies and law enforcement agencies may face resource constraints that limit their ability to effectively combat these scams.

In the present interconnected digital era, it is imperative for the enforcement authority and banks to utilise the potential of artificial intelligence (AI) and machine learning (ML) technology, as these tools have proven to be highly efficient in combating fraudulent activities. (O'Brien, 2023). Computer science's artificial intelligence (AI) field seeks to replicate human intelligence in machines. Investigators and analysts use it to foresee, identify, and stop fraudulent activity in real-time. Conversely, machine learning (ML), a branch of artificial intelligence, allows computers to learn from historical data without explicit programming, which aids in identifying changing fraudulent patterns. The enforcement authority and banking industry can better understand and anticipate criminal patterns and behaviours and, consequently, prevent or lessen the impact of fraud by combining sophisticated AI and ML technologies with cross-industry data sharing (O'Brien, 2023).

5. Institutional Framework

A specific agency to address the core matter in the Macau scam in a holistic manner, the National Scam Response Centre (NSRC) was established in October 2022. The NSRC is a collaborative effort between the Anti-Financial Crime Centre (NFCC), the Royal Malaysia

Asian Journal of Law and Governance
e-ISSN: 2710-5849 | Vol. 6, No. 3, 11-21, 2024
http://myjms.mohe.gov.my/index.php/ajlg

Police, Bank Negara Malaysia (BNM), the Malaysian Communications and Multimedia Commission (MCMC), financial institutions, and telecommunications companies. The NSRC specialises in online financial fraud, such as phishing scams, Macau scams, malware attack scams, parcel scams, and love scams. The NSRC has established a 997 hotline to help combat scams, including the Macau scam. The hotline operates daily between 8 am to 8 pm, including public holidays. In the first four months after its establishment, the NSRC 997 hotline received 16,752 reports of scam calls involving losses of nearly RM40 million (Muhammad, 2023). As a result, the police have opened 751 fraud-related investigations under Penal Code section 420 and 24 cases under the Prevention of Money Laundering, Prevention of Terrorism Financing and Proceeds from Illegal Activities Act 2001 (Harun et al., 2023).

The primary function of the Commercial Crime Investigation Department (CCID) Royal Malaysia Police is to arrest, investigate and prosecute white-collar criminals who commit fraud, criminal breach of trust, cybercrime forgery and others, whether these activities are carried out by individuals or syndicates (CCID portal, n.d.). The CCID Scam Response Center hotline, also operates daily and offers support to those who believe they have been the target of a scam. The centre provides advice on how to proceed and can assist in verifying the authenticity of suspicious contacts. Moreover, the CCID-operated Semak Mule platform enables the general public to verify if bank account numbers or phone numbers have been flagged for suspicious or fraudulent behaviour. CCID also maintains an official Facebook page where they share updates regarding scam alerts, preventive measures, and public awareness campaigns.

Bank Negara Malaysia, in its capacity as the central bank of Malaysia, has implemented supplementary measures and enhanced security protocols within the banking sector to address the operational methods employed by recent financial scams. Starting from January 1, 2019, banks are obligated to include any cash transactions that surpass RM25,000 in their daily threshold report. In the past, the threshold for reporting cash transactions stood at RM50,000. The present practice is timely and possesses the potential to be utilised as an additional measure in countering fraudulent activities in the Macau scam. According to the Association of Banks in Malaysia (ABM), the banking sector is anticipated to completely execute the five essential steps announced by Bank Negara Malaysia to tackle online scams by June 2023 (Muhammad, 2023). These key measures are first, migrating from SMS to one-time passwords (OTPs) to a more secure authentication method; second, strengthening the rules and triggers for blocking suspicious transactions; third, verification and a cooling-off period for first-time enrolment in e-banking services or the use of a secure device; fourth, allowing only one mobile or secure device to be registered for transaction verification purposes; and finally, a dedicated complaint hotline that is available around the clock to report incidents or suspicions of scams (Muhammad, 2022).

The Malaysian Communications and Multimedia Commission (MCMC) also plays a critical role in combating the Macau scam through various strategic actions and collaborations. As of September 2023, they have successfully blocked over 2.6 billion suspected scam calls and terminated 134 phone numbers associated with fraudulent activities (Tan et al., 2023). MCMC has also stepped up its efforts by working with other countries. MCMC and Singapore's Infocomm Media Development Authority (IMDA) signed a Memorandum of Understanding (MOU) in February 2024 to work together better against telecommunication scams across borders (Chiew, 2024). The agreement aims to make it easier to share strategic information, coordinate actions taken by regulators, and support educational programs that keep people safe from scams. In addition, MCMC also actively engages in multiple campaigns to raise

Asian Journal of Law and Governance
e-ISSN: 2710-5849 | Vol. 6, No. 3, 11-21, 2024
http://myjms.mohe.gov.my/index.php/ajlg

awareness about the prevalence of scams, fraud, and consumer protection rights (MCMC, 2022).

One essential component of combating financial scams is educating the general public about the various con tricks perpetrated by criminals as well as the preventative measures that individuals can take to lessen their likelihood of falling prey to these scammers. According to Mohd Yunus (2022), BNM, the financial sector, and law enforcement will continue to work to improve the effectiveness of public awareness campaigns and information dissemination. Many different channels and platforms have been used to educate and raise consumer awareness about financial scams. For example, BNM and banking institutions have provided scam alert tips on their websites, while the police have been actively educating consumers about scams through the social media. On the other hand, in order to effectively address and reduce financial crime, it is necessary for all relevant stakeholders to collaborate. It is imperative that consumers take responsibility for their actions and engage in self-protection against fraudulent activities.

6. Implication, Recommendation dan Future Directions

The implications of this paper can be applied to various groups, including regulators, financial industry, consumer movements and consumers in general. Consumers should always be alert and prioritise self-protection in daily activities. It is crucial to be extra cautious when receiving calls, and consumers should be more sceptical of unsolicited calls. In addition, consumers could use call-blocking and filtering tools and install apps such as Truecaller to identify unknown calls and block spam calls and text messages. Mainstream and social media platforms, including Instagram and Facebook, are news sources and information regarding scam activities. For example, the Central Bank and the Commercial Crime Investigation Department (CCID) for example, are active on Facebook, Instagram, and TikTok to convey awareness and constantly remind to the public about the latest modus operandi of scammers.

Furthermore, the implication to regulators, the financial industry and consumer movements play a crucial role in addressing scams by providing consumer education. Their endeavours to enhance awareness and furnish resources are crucial in safeguarding consumers from deceitful activities. Through collaboration with consumer education, they establish a comprehensive strategy for preventing scams that empowers consumers and ensures the maintenance of a secure and reliable communication platform. For example, the financial alerts published by the banks on their websites and apps advised the public to stay vigilant with the latest warnings and prevention tips regarding the modus operandi of scammers. In addition to safeguarding the consumers, these initiatives also boost credibility and trust in the regulators and the government.

The issue of law enforcement in tackling phone scams is complex and requires a comprehensive strategy. The Macau scams frequently function as components of worldwide, organised criminal networks. Addressing these issues is a highly demanding task that necessitates well-coordinated and comprehensive actions on a global level. Tackling this worldwide phone scam syndicate necessitates a comprehensive strategy that encompasses international collaboration, unified laws, technological remedies, and ongoing public awareness campaigns. This issue is intricate, but it requires a synchronised global effort to safeguard susceptible consumers across the globe.

In regard to recommendations and future directions, the enforcement authority and banking industry must harness the power of artificial intelligence (AI) and machine learning (ML) technology in today's connected digital world. These tools have been shown to be extremely effective in the fight against fraud. By combining sophisticated AI and ML technologies with cross-industry data sharing, the enforcement authority and banking industry can better understand and anticipate criminal patterns and behaviours, and consequently, prevent or lessen the impact of fraud. Apart from that, although the Central Bank has issued additional countermeasures and more security to the banking industry, a novel approach needs to be considered. A fair compensation and protection model that efficiently defends consumers against scammers has to be further studied.

7. Conclusion

The Macau scam has caused substantial financial devastation for countless individuals worldwide. Law enforcement agencies are greatly concerned about the widespread occurrence of such crimes. The pertinent authorities are intensifying their endeavours to counteract fraudulent activities. Nevertheless, the current consumer protection framework regarding phone scams can be enhanced by bolstering applicable legislation and enhancing the enforcement system. Coordinating efforts between jurisdictions and regulatory agencies is crucial to combat AI-enabled phone scams effectively. In addition, collaboration with technology companies is crucial to detect and prevent phone scams and to share information and data to track and identify scammers.

Acknowledgements
This work is funded by the Fundamental Research Grant Scheme, FRGS/1/2022/SS09/UPM/02/01.

References

Adib, P. & Arfa, Y. (2020, August 17). Online face mask scams raked in RM18 million during MCO. *New Straits Times*. https://www.nst.com.my/news/nation/2020/08/617270/online-face-mask-scams-raked-rm18-million-during-mco

Akhbar, S. (2021, 19 Oktober). Macau Scam sudah di tahap krisis nasional? *Bernama.* https://www.bernama.com/bm/tintaminda/news.php?id=1891294

Australian Competition & Consumer Commission (2021, September 27). Losses reported to Scamwatch exceed $211 million, phone scams exploding. [Media Release]. https://www.accc.gov.au/media-release/losses-reported-to-scamwatch-exceed-211-million-phone-scamsexploding.

Alarming increase in scam calls found in Thailand. (2023, April 8). *The Nation. https://www.nationthailand.com/thailand/general/40026460*

Bidgoli, M. & Grossklgs, J. (2017). "Hello. This is the IRS calling:" A case study on scams, extortion, impersonation, and phone spoofing. *2017 APWG Symposium on Electronic Crime Research (eCrime)*, Scottsdale, AZ, USA, pp. 57-69, doi: 10.1109/ECRIME.2017.7945055.

Chiew, S. Singapore and Malaysia sign MOU to tackle scams across telecommunications channel. (2024, Feb 26). *The Edge.* https://www.theedgesingapore.com/news/telecommunications/singapore-and-malaysia-sign-mou-tackle-scams-across-telecommunications

Commission for Communications Regulation. (2023). Combatting scam calls and text. https://www.comreg.ie/media/2023/06/Consultation.pdf

Consumers International. (2020). *Social media scams: Understanding the consumer experience to create a safer digital world*. https://www.consumersinternational.org/media/293343/social-media-scams-final-245.pdf

Conway, L. (2021). *Consumer protection: Online scams*. House of Commons Library Briefing Papers (HC 2021-9214). Retrieved from https://library-guides.ucl.ac.uk/harvard/parliamentary-paper

European Commission. (2020). *New Consumer Agenda. Strengthening consumer resilience for sustainable recovery*. https://www.europeansources.info/record/new-consumer-agenda-strengthening-consumer-resilience-for-sustainable-recovery/

Farahanim, M.A. & Tengku Elena, T.M. (2023). Anatomy of phone scams: victims' recall on the communication phrases used by phone scammers. Proceedings of the International Conference on Communication and Media 2022 (i-COME 2022), 498-509. https://doi.org/10.2991/978-2-38476-098-5_43

Gainsbury, S.M. (2019). Identifying risky internet use: Linking negative internet experiences to specific online behaviour. *New Media and Society*, 21(6), 12-32.

Goh, P.P. (2019, August 9). Coaches keep Macau scam syndicates 'a few steps ahead of the law'. *New Straits Times*. https://www.nst.com.my/news/nation/2019/08/511435/coaches-keep-macau-scam-syndicates-few-steps-ahead-law

Hancock, J. (2022). *Fighting Fraud: Breaking the Chain*. https://www.finextra.com/blogposting/23277/fighting-fraud-breaking-the-chain

Harun, H.N., Sallehudin, Q, & Mohamed Radhi, N.A. (2023, February 15). Anti-scam hotline logs almost 17,000 reports, involving RM40m losses, since October. *New Straits Times,* https://www.nst.com.my/news/nation/2023/02/880108/anti-scam-hotline-logs-almost-17000-reports-involving-rm40m-losses

HM Government. *Fraud Strategy: Stopping Scams and Protecting the Public*. (2023). CP839.

House of Lords and the Digital Fraud Committee. (2022). *Fighting Fraud: Breaking the Chain*. HL Paper 87.

Huang, T. H. D., Yu, C. M., & Kao, H. Y. (2018). Data-Driven and Deep Learning Methodology for Deceptive Advertising and Phone Scams Detection. In *Proceedings - 2017 Conference on Technologies and Applications of Artificial Intelligence, TAAI 2017* (pp. 166-171). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/TAAI.2017.30

Hubbard, T., Reeves, A. & Birch, A. (2023, May 16*). UK fraud strategy: loud bark, little bite?* https://www.regulationtomorrow.com/eu/uk-fraud-strategy-loud-bark-little-bite/

Indonesia named third-worst spammed country in the world. (2019, December 7). *The Jakarta Post. https://www.thejakartapost.com/life/2019/12/07/indonesia-named-third-most-spammed-country-in-the-world.html*

Jabatan Siasatan Jenayah Komersil. (2022, 6 Januari). *Kenyataan Media Pengarah Jabatan Siasatan Jenayah Komersil Modus operandi baharu penipuan "Macau Scam."* Facebook. https://www.facebook.com/JSJKPDRM/photos/pcb.379400100624641/379405807290737/

Lam, A. (2019, November 29). What is the 'Macau scam'? *Macau Daily Times*. Available at: https://macaudailytimes.com.mo/what-is-themacau-scam.

Lu, H. Y., Chan, S., Chai, W., Lau, S. M. & Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime*

Prevention and Community Safety, *22*(4), 313–330, 2020, DOI: https://doi.org/10.1057/s41300- 020-00098-3

Macau Scams: Msians duped out of RM256 million this year. (2020, November 16). *New Straits Times*. https://www.nst.com.my/news/nation/2020/11/641653/macau-scams-msians-duped-out-rm256-million-year

Malaysian Communications and Multimedia Commissions. (2022). Integrated annual report. https://www.mcmc.gov.my/skmmgovmy/media/General/Report/MCMC-AR-2022_Eng.pdf

Mohd Yunus, N.S. (2022, September 26). *Governor's Speech at the Launching of Financial Crime Exhibition*. Bank Negara Malaysia. https://www.bnm.gov.my/-/financial-crime-exhibition-speech-en

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, *59*(2), 186-209.

Muhammad Basir, R. (2020, October 12). Expert: Important to recognise modus operandi of Macau scams. *Bernama*. https://www.bernama.com/en/features/news.php?id=1888770

Muhammad, S. (2022, December 13). Banks expected to fully implement BNM's measures to combat online scams by June 2023. *The Edge. https://theedgemalaysia.com/article/banks-expected-fully-implement-bnms-measures-combat-online-scams-june-2023-%E2%80%94-abm*

Muhammad, S. (2023, March 27). Losses from financial scams totalling RM39m reported from October 2022 to January 2023, says Anwar. *The Edge. https://theedgemalaysia.com/node/660994*

Nasaruddin, N.I. & Zulkefly, A.Z. (n.d.). *Legal Implications/Remedies in Relation to Common Business Scams in 2020.* https://www.azmilaw.com/insights/legal-implications-remedies-in-relation-to-common-business-scams-in-2020/

Norris, G., & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, *169*(1), 109-847.

Nurul Hidayah, B. (2020, Mac 29). Hati-hati sindiket penipuan KWSP. *Harian Metro*. https://www.hmetro.com.my/mutakhir/2020/03/559890/hati-hati-sindiket-penipuan-kwsp

OECD (2020). *Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy*. www.oecd.org/finance/Financial-Consumer-Protection-Policy

Peter, Z. (2023, December 23). Southeast Asian scam hubs drawing global scrutiny as reach grows. *Voanews.* https://www.voanews.com/a/southeast-asian-scam-hubs-drawing-global-scrutiny-as-reach-grows-/7409758.html

Phone scams. (2024, March). *Which?* https://www.which.co.uk/consumer-rights/advice/phone-scams-aL1Yy5L9Utl4

Shaari, A. H., Kamaluddin, M. R., & Paizi, W. F. (2019). Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims. *GEMA Online Journal of Language Studies*, *19*(1), 97–115, DOI: https://doi.org/10.15520/jro.v6i 9.23.

Tan, B. (2023, December 19). Scams on the rise in Malaysia: Survey finds phone calls most popular route, followed by WhatsApp. *Malay Mail*. https://www.malaymail.com/news/malaysia/2023/12/19/scams-on-the-rise-in-malaysia-survey-finds-phone-calls-most-popular-route-followed-by-whatsapp/108274

Tan, T., Vethasalam, R., & Yusof, T.A. 2.6 billion scam calls blocked by MCM so far. (2023, Oct 18). *The Star*. https://www.thestar.com.my/news/nation/2023/10/18/26-billion-scam-calls-blocked-by-mcmc-so-far

Tang, L. (2024, February 18). Scam cases in Singapore jumped almost 50% in 2023, most victims fell for job, e-commerce cons. *Channel News Asia*. https://www.channelnewsasia.com/singapore/scams-2023-increase-50-percent-job-e-commerce-measures-4128051

United Nations Conference on Trade and Development. (2018). *Manual on Consumer Protection.* https://unctad.org/webflyer/manualconsumer-protection

Yeoh, A. LHDN warns of SMS scam targeting Bantuan Prihatin Nasional recipients. (2020, April 3). *The Star*. https://www.thestar.com.my/tech/tech-news/2020/04/03/lhdn-warns-of-sms-scam-targeting-bantuan-prihatin-nasional-recipients

Wan Sulaiman, W.S., Murad, F.A., Mat Saat, G.A., Khairudin, R., Mohamed Mokhtar, D.M., Mariamdaran, S., Shaari, A.H. & Kamaluddin, M.R. (2022). Development and validation of victimisation risk inventory (SVR-I) among Malaysian population. *Journal of Legal, Ethical and Regulatory Issues, 25*(S5), 1-15.

Whitty, M.T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victms. *European Journal on Criminal Policy and Research*, 26, 399-409.

Williams, T. (2023, April 12). Expert says AI scams are on the rise as criminals use voice cloning, phishing and technologies like ChatGPT to trick people. *Australian Broadcasting Corporation.* https://www.abc.net.au/news/2023-04-12/artificial-intelligence-ai-scams-voice-cloning-phishing-chatgpt/102064086

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72(1), 412-421.