JSSMR
JOURNAL OF SOCIAL SCIENCE
AND MULTIDISCIPLINARY RESEARCH

Received: 5 March 2024
Accepted: 31 March 2024
Published Online: 31 March 2024
Reviewing Editor: Waiphot Kulachai, Suan Sunandha Rajabhat University, Bangkok, Thailand

REVIEW ARTICLE

Thailand's Legal Framework Against Call Center Crimes

Pakin Wangsathitham[1,*]

[1]Office of The National Broadcasting and Telecommunications Commission, Bangkok, Thailand; pakin4949@gmail.com
* Correspondence: pakin4949@gmail.com

Abstract

Call center crimes have emerged as a significant global challenge, characterized by their diversity and complexity. This study explores the various forms of illegal activities associated with call centers, including fraud, identity theft, extortion, money laundering, human trafficking, unauthorized access to data, and market manipulation. Utilizing a comprehensive review of recent literature and case studies, the paper examines the operational vulnerabilities of call centers that criminals exploit, the socio-economic impacts of these crimes, and the existing legal frameworks aimed at addressing them, with a particular focus on Thailand. The findings reveal that despite the efforts to combat these crimes through legal and regulatory measures, challenges persist due to the transnational nature of the operations and the sophistication of the tactics employed. The paper proposes a set of recommendations, emphasizing the need for stronger regulatory frameworks, technological advancements in fraud detection and identity verification, public awareness campaigns, and international cooperation to enhance the effectiveness of the response to call center crimes. The insights offered aim to assist policymakers, law enforcement agencies, and industry stakeholders in developing more effective strategies for prevention, intervention, and legal action against call center-related criminal activities.

Keywords: call center; cybercrime; law enforcement; legal framework; organized crime

1. Introduction

Call center crime encompasses a broad spectrum of illegal activities facilitated through or targeting call centers, involving fraud, identity theft, data breaches, and various forms of cybercrime. Scholars offer diverse perspectives on the operational dynamics of call centers, which can indirectly shed light on the vulnerabilities and criminal opportunities within these settings. For instance, Brown et al. (2005) provides a statistical analysis of call center operations from a queueing theory perspective, highlighting the complexity of managing arrivals, customer patience, and service durations, which could be exploited by criminals aiming to disrupt or deceive call center functions. Akşin, Armony, and Mehrotra (2007) delve into the operational challenges exacerbated by technological advancements, emphasizing the evolving nature of call center operations that could be susceptible to cybercrime due to increased digitalization and reliance on information technology. Anderson (2015) explores the social implications of call center employment for deported and returning migrants, suggesting that the socioeconomic context of call centers can influence the potential for criminal activities, including fraud and exploitation.

The global landscape of call center crimes has undergone significant transformation, propelled by advancements in technology and shifts in criminal tactics. Notably, the surge in identity fraud has emerged as a critical concern, impacting millions worldwide and resulting in considerable financial losses, thereby calling for an advanced and strategic law enforcement response to curb this trend (McMahon, Bressler, & Bressler, 2016). Despite the alarming rise in cybercrime reports, a closer examination and normalization of these statistics reveal a more nuanced narrative, suggesting that the vast expansion of the digital domain has not necessarily led to a proportionate increase in cybercrime, thereby challenging the prevailing narrative of a digital realm besieged by insecurity (Jardine, 2015). The advent of the COVID-19 pandemic marked a pivotal moment, exacerbating the situation by providing fertile ground for cybercriminals to exploit the increased dependency on digital platforms, leading to a notable spike in online fraud and hacking activities. This period underscored the pressing need for robust cybersecurity measures and heightened vigilance among individuals and organizations alike (Park et al., 2020). Furthermore, the emergence of sophisticated cybercrime forms such as ransomware attacks and sextortion has underscored the dynamic and evolving nature of cyber threats. These developments highlight the critical need for ongoing adaptation in cybersecurity strategies and the importance of fostering international collaboration to effectively combat these pervasive challenges (McMahon, Bressler, & Bressler, 2016). The diversity and sophistication of cybercrimes across different regions accentuate the necessity for targeted cooperation and the deployment of cutting-edge countermeasures to protect the digital landscape, ensuring the security and trustworthiness of digital communications and transactions in an increasingly interconnected world.

The impacts of call center crime encompass a wide range of consequences, affecting not only the direct victims but also the broader operational and psychological landscape of call center environments and beyond. For example, experimental studies on call center interactions, such as those examining the effects of disclaimers on callers' willingness to disclose information, suggest nuanced impacts on caller behavior and the potential for information withholding, which could affect the effectiveness of call centers in addressing issues like terrorism or violent extremism (Williams, Bélanger, Horgan, & Evans, 2019). Furthermore, research into the general impacts of crime on health and health services highlights the substantial risks and costs associated with criminal activities, suggesting that victims of call center crimes may also experience significant physical and psychological health impacts, thereby generating additional demand for health services (Robinson & Keithley, 2000). Moreover, the operational efficiency of call centers can be severely compromised by criminal activities, leading to increased role stress among employees and potentially affecting their performance and satisfaction (de Ruyter, Wetzels, & Feinberg, 2001). Employee well-being is a critical concern in call centers, often perceived negatively due to factors such as job design, performance monitoring, and HR practices. Criminal activities exacerbate these issues, contributing to anxiety, depression, and reduced job satisfaction, highlighting the need for supportive team leader roles and high control over work methods to mitigate the negative impacts (Holman, 2002). On a broader scale, organized crime activities, including those targeting or involving call centers, pose significant public health concerns. The income-generating activities of organized crime, ranging from traditional vice activities to newer areas such as human trafficking and the sale of counterfeit products, affect community health and safety, indicating the complex interplay between call center crimes and wider societal issues (Reynolds & McKee, 2010).

The recent developments in call center crimes in Thailand and their global expansion reflect a growing concern over cyber scams and related criminal activities. The trend has seen human trafficking for the purpose of staffing scam call centers, extending from Southeast Asia to regions such as South America and the Middle East. This global spread underscores the evolving and increasingly complex nature of call center crimes, encompassing a wide array of illegal activities including cyber scams, human trafficking, and digital fraud (Jones, 2023). In 2022, Thai authorities took significant steps to combat these crimes, arresting 166 suspects from eight foreign call center gangs. This action was part of a broader crackdown on cybercrime in Thailand, targeting not only scam call centers but also illegal account trading and gambling websites. These efforts indicate a proactive approach by Thai authorities in addressing the multifaceted threats posed by call center-related crimes. However, the ongoing evolution of these criminal activities, coupled with their expanding geographical footprint, highlights the persistent challenge they pose, necessitating continuous and coordinated international efforts to effectively mitigate their impact.

Hence, this study aims to explore the various categories of crimes associated with call centers, their repercussions, and the legal measures implemented to counteract these offenses. The insights garnered from this research are intended to be advantageous for individuals involved in policy development and law enforcement entities. By delving into the nuances of call center-related criminal activities, this paper seeks to provide a comprehensive overview that can inform more effective strategies for prevention, intervention, and legal action against such crimes. The outcomes of this investigation could serve as a valuable resource for shaping policies and enhancing the capabilities of law enforcement agencies in tackling the complex challenges posed by call center crimes.

2. Categories of Call Center Crime

Categories of call center crime encompass a broad spectrum of illegal activities facilitated through or targeting call center operations. These categories can be broken down into several key areas, each representing unique challenges for law enforcement and policymakers:

2.1 Fraud and Scams

The category of fraud and scams in call centers includes a diverse array of deceptive practices aimed at unlawfully obtaining money or personal information from individuals. These practices have evolved significantly with the advancement of technology, leading to the emergence of sophisticated schemes such as IRS scams, lottery scams, tech support scams, and phishing attempts. In these scams, perpetrators often impersonate legitimate organizations to exploit victims, causing financial loss, identity theft, and a host of other fraudulent activities. Recent research has highlighted the growing prevalence of scam calls, which have become a major concern resulting in financial losses, identity theft, and other forms of fraud. Hong, Connie, and Goh (2023) proposed a machine learning-based approach for scam call classification and detection, utilizing natural language processing and deep learning techniques to identify scam conversations with an accuracy of 85.61%. Similarly, Kale et al. (2021) developed a system to classify fraudulent calls by analyzing call transcripts through machine learning techniques, achieving accuracies up to 97.21% with their models. Malhotra, Arora, and Bathla (2023) presented an overview of AI-based fraud detection techniques, demonstrating high accuracy in identifying potential indicators of fraud or spam. These studies underscore the critical role of technological advancements in combating call center fraud and scams. By leveraging machine learning and artificial intelligence, researchers and practitioners are developing more effective tools to detect and prevent fraudulent activities. These efforts are essential for protecting individuals and organizations from the financial and emotional impacts of call center crimes.

2.2 Identity Theft

Identity theft in call centers involves operations where criminals exploit personal information to commit fraud, such as opening unauthorized accounts, making purchases, or other forms of financial fraud under the victim's name. This crime has seen significant growth due to the integration of technology into everyday life, making the psychological and financial impact on victims particularly devastating. Lohr (2019) highlights that identity theft can be more damaging than other frauds, like credit card theft, as it may involve the thief opening new accounts in the victim's name, leading to a long and costly recovery process for the victim. Similarly, Kahn and Liñares-Zegarra (2016) explored how identity theft incidents influence consumer payment choices, indicating shifts in the adoption and usage of certain payment methods following identity theft experiences. Helser and Hwang (2021) provide a comprehensive review of identity theft, examining the human element of the crime, the techniques used by perpetrators, and the countermeasures developed to combat these activities. Cassim (2015) discusses the legal challenges and solutions introduced in various countries to combat identity theft, underscoring the need for a multi-faceted approach to address this issue effectively. Farina (2015) and Kempen (2016) explore the various types of identity theft, including medical, financial, and child identity theft, highlighting the prevalence of the crime and its costs to victims in terms of money, stress, and emotional distress.

2.3 Extortion

Extortion through call centers and ransomware attacks has rapidly evolved into a sophisticated cyber threat, with criminals leveraging digital platforms to execute schemes that have caused estimated damages of $1 billion. Studies by O'Kane, Sezer, and Carlin (2018) and Mansfield-Devine (2016) illustrate the transition from early ransomware attempts to advanced malware campaigns, highlighting ransomware's status as the biggest cyber-threat in Europe, particularly targeting vulnerable sectors like healthcare. Malkawe et al. (2019) emphasize the pervasive threat ransomware poses across modern digital infrastructures, from IoT devices to healthcare systems, underscoring the necessity of comprehensive vulnerability assessments. Furthermore, Sharmeen et al. (2020) and Keshavarzi and Ghaffary (2020) discuss the need for robust digital extortion defenses, advocating for deep learning-based adaptive approaches and a dedicated ransomware attack chain, I2CE3, to enhance the cybersecurity community's readiness against these extortion tactics. These insights collectively underline the urgency of advancing defensive technologies and strategies to protect against the evolving landscape of ransomware and cyber extortion threats.

2.4 Money Laundering

Illicit call centers have increasingly become instrumental in money laundering activities, where criminals use these platforms to disguise the origins of illegally obtained funds by channeling them through seemingly legitimate transactions. Colladon and Remondi (2021) illustrate the application of network analytic techniques in detecting and preventing money laundering activities, showcasing how social network metrics can predict risk profiles of clients involved in financial operations, thus aiding in the identification of suspicious activities. Similarly, Teichmann (2020) provides insights into the concrete techniques employed in Europe for laundering money, revealing that money laundering is not necessarily costly for criminals and can generate significant profits, thereby highlighting the sophistication and low barriers to entry for engaging in such illicit activities. Moreover, Chen et al. (2018) emphasize the role of machine learning in enhancing anti-money laundering (AML) solutions, specifically in detecting suspicious transactions, indicating a shift towards more technologically advanced methods to counteract these criminal endeavors. The utilization of advanced analytics and machine learning not only improves the detection of money laundering schemes but also addresses the need for innovative solutions to combat the evolving tactics of criminals using call centers as fronts for their illegal operations.

2.5 Human Trafficking and Labor Exploitation

The involvement of call centers in human trafficking and labor exploitation presents a complex challenge that spans legal, ethical, and health domains. Research by Kiss et al. (2015) highlights the severe mental health outcomes, including depression, anxiety, and PTSD, faced by survivors, particularly children and adolescents in the Greater Mekong Subregion, underlining the urgent need for comprehensive support services. Coverdale et al. (2016) advocate for the integration of human trafficking education within psychiatric and medical training to better equip healthcare professionals to identify and assist victims, emphasizing the critical role of the healthcare sector in addressing this global health concern. Weatherburn (2021) and Berket (2015) discuss the legal complexities and the need for clearer definitions and stronger policy frameworks to effectively combat labor exploitation and trafficking, highlighting the importance of international cooperation and the involvement of the private sector in developing effective responses. Zimmerman and Kiss (2017) further stress the significance of adopting a public health policy framework to guide the global response to trafficking, illustrating the pervasive nature of this issue and the necessity for a multifaceted approach that includes prevention, protection, and prosecution strategies. These insights collectively underscore the imperative for a coordinated effort that spans legal reform, education, and international collaboration to protect vulnerable individuals from the scourge of human trafficking and labor exploitation.

2.6 Unauthorized Access and Cybercrimes

Call centers have become significant vectors for cybercrimes, with criminals deploying sophisticated methods to gain unauthorized access to computer systems and networks, spread malware, execute denial of service (DoS) attacks, and steal sensitive corporate data. McMahon, Bressler, and Bressler (2016) outline a variety of cybercrimes, including identity fraud and theft of money or data, which have caused significant financial impact and highlighted the necessity for advanced technological and law enforcement strategies to counter these threats. The COVID-19 pandemic has further escalated the risk, with Buil-Gil et al. (2020) reporting an increase in cyber-dependent crimes, particularly frauds associated with online shopping and auctions, and hacking of social media and email accounts, underscoring the displacement of crime opportunities from physical to online environments. Al-Khater, Al-Maadeed, Ahmed, Sadiq, and Khan (2020) provide an intensive review of cybercrime detection and prevention techniques, highlighting the role of machine learning in identifying threats to privacy and security in computer systems. Defossez (2021) discusses the challenges in regulating cybercrimes due to the continuous development of new technologies and the anonymity provided by the internet, indicating an enforcement gap that allows cybercriminals to operate with near impunity. These studies collectively emphasize the critical need for ongoing development of cybersecurity measures, law enforcement strategies, and international cooperation to effectively combat unauthorized access and cybercrimes facilitated through call centers.

2.7 Market Manipulation and Investment Scams

The phenomenon of market manipulation and investment scams through call centers, as highlighted in recent studies, underscores the complexity and sophistication of these fraudulent schemes. DeLiema, Shadel, and Pak (2020) profile the typical victims of such scams, often characterized by a higher socioeconomic status and lured by the promise of unreasonable returns, exposing a critical need for targeted investor education and awareness. Lewis (2018) provides an insight into the subversive manipulation of development apparatuses in Jamaica through lottery scamming, illustrating the broader socioeconomic impacts and the inversion of traditional capital flows between nations. Siering, Clapham, Engel, and Gomber (2017) emphasize the importance of developing a comprehensive taxonomy for financial market manipulations to enhance the effectiveness of automated fraud detection systems, highlighting the role of speculative trading and new trading technologies in facilitating these crimes. Wood et al. (2018) and Lin (2017) further shed light on the psychological and technological dimensions of these scams, demonstrating how perceived benefits and the misuse of electronic networks and artificial intelligence contribute to the victimization process, thus underscoring the urgent need for regulatory policies and protective measures to safeguard the financial market's integrity and investor trust.

3. Consequences of Call Center Crime

The consequences of call center crimes extend significantly beyond the immediate victims, impacting social and economic dimensions, public health, and community trust. The economic shock and subsequent crime reduction potential of financial assistance, as examined by Palmer, Phillips, and Sullivan (2019), illustrate how such interventions can mitigate the social consequences of economic distress, potentially reducing the allure of criminal activities facilitated through call centers. Anderson (2015) delves into the social implications of call center crimes, particularly focusing on deported and returning migrants in Mexico City, highlighting the broader issues of criminalization and marginalization of vulnerable populations. The effect of call center crimes on public trust and safety, as discussed by Williams, Bélanger, Horgan, and Evans (2018), points to the delicate balance between ensuring confidentiality and the need for law enforcement interventions in sensitive cases, indicating the complex interplay between crime prevention and individual rights. The outbreak of COVID-19 in a South Korean call center reported by Park et al. (2020) underscores the vulnerability of such environments to health crises, further complicating the challenges posed by call center crimes. These insights collectively highlight the multifaceted consequences of call center crimes, demanding a nuanced and comprehensive approach to address the social, economic, and health-related impacts. Mitigating these effects requires targeted social interventions, robust legal frameworks, and international cooperation to protect vulnerable populations and maintain public trust and safety.

4. Legal Framework Against Call Center Crime

In Thailand, addressing call center crimes involves a complex legal framework that emphasizes both the prosecution of criminal activities and preventative measures within the telecommunications industry. Call center gangs commit offenses characterized as "transnational organized crime" where the offenses must be severe, punishable by imprisonment of at least 4 years as defined by the United Nations Convention against Transnational Organized Crime and the Act on Prevention and Suppression of Participation in Transnational Organized Crime, B.E. 2556 (2013).

However, the offenses committed by these individuals can only be penalized based on the offense of fraud under Section 341 of the Criminal Code, which stipulates a penalty of imprisonment not exceeding 3 years, or a fine not exceeding 60,000 baht, or both. Therefore, the basis of the offense used to punish call center gangs does not correspond to the severity of the crime. When the offenses of call center gangs pose a significant threat to the country's economic system, worth a vast amount. Moreover, the severity of a crime should be measured by its harm, the victims affected by the crime, as well as the morality and wrongfulness of the crime itself. In the United States, similar offenses, such as extortion for credit transactions and email fraud, are designated as offenses under the Organized Crime Control Act of 1970. However, the punishment for fraud offenses, with a maximum imprisonment of only 3 years, is low compared to the severity of the crime or the value of the assets that call center gangs obtain from deceiving victims, making it worthwhile for call center gangs to continue their criminal activities. The penalty rate for such offenses does not match the severity that would lead to an offense within a transnational organized crime organization as defined by the Act on Prevention and Suppression of Participation in Transnational Organized Crime, B.E. 2556 (2013), posing a significant problem in law enforcement's effectiveness in suppressing offenders in transnational organized crime.

The enforcement of criminal laws targets activities through the designation of offenses and the application of state criminal policy, yet it faces challenges in effectively arresting and eradicating criminal elements due to the sophisticated and elusive nature of these operations. Criminals often operate without a fixed address, utilizing advanced deceptive methods that complicate efforts to trace and prosecute them. As a result, the current legal approach, which predominantly relies on post-incident prosecution and requires substantial evidence for legal action, has shown limited success in reducing the prevalence of call center gangs. The problem is not unique to Thailand; similar challenges are encountered internationally, where there is a shift towards a more proactive stance focusing on prevention rather than solely on suppression. Effective strategies include the involvement of both public and private sectors in developing actionable and measurable plans to prevent such criminal activities. For instance, in countries like the United Kingdom and Australia, concerted efforts between the state and telecommunications providers have led to the implementation of annual action plans and legislative measures aimed at monitoring and verifying phone number identities to prevent misuse. These initiatives are complemented by public awareness campaigns designed to educate citizens about the risks of call center scams and how to protect themselves. This integrated approach underscores the importance of a multi-faceted legal framework that combines rigorous enforcement of criminal laws with proactive preventative measures and public education. By fostering collaboration among telecommunications companies, law enforcement agencies, and the broader community, Thailand can enhance its ability to combat call center crimes, mitigate damages, and safeguard the public against these evolving threats.

5. Recommendations

To effectively combat the issue of call center crimes, a comprehensive and multi-faceted approach is required. This approach should not only focus on legal and regulatory measures but also on technological solutions and public awareness initiatives. Below are expanded suggestions and additional suitable countermeasures:

1. Strengthening Regulatory Frameworks: Regulatory measures in the telecommunications industry need to be fortified. This involves revising existing laws and introducing new regulations that specifically address the unique challenges posed by call center crimes. Telecommunications service providers should be mandated to implement stringent customer verification processes, maintain detailed call logs, and actively monitor for suspicious activities.

2. Verification and Identity Confirmation: Implementing advanced verification and identity confirmation technologies can help prevent fraudsters from obtaining service under false pretenses. Biometric verification, two-factor authentication, and digital ID checks should become standard practices for all telecommunications providers to ensure that only legitimate customers can access services.

3. Developing a One Stop Service System: Establishing a centralized platform where individuals can report scam calls, receive information on known scams, and learn protective measures could significantly enhance public awareness and resilience against call center crimes. This platform could also serve as a hub for coordinating responses between law enforcement, regulatory bodies, and telecommunications providers.

4. Enhanced Detection and Blocking Technologies: Service providers should invest in technology that can detect, track, and block scam calls in real-time. Artificial intelligence and machine learning algorithms could analyze call patterns and flag potential scam activities, preventing them from reaching potential victims. Sharing information about suspicious numbers across providers can also help in creating a more comprehensive defense against these crimes.

5. Amending the Criminal Code for Fraud Offenses: The penalties for fraud offenses, especially those committed through call centers, should be revised to reflect the severity and impact of these crimes. Higher penalties, including longer

imprisonment terms and larger fines, could deter individuals from engaging in such activities.

6. Public Awareness Campaigns: Raising public awareness about call center crimes is crucial. Regular campaigns, educational programs, and easily accessible resources can inform the public about common scams, how to recognize potential fraud, and steps to take when targeted.

7. International Cooperation: Since call center crimes often cross national borders, international cooperation is essential for tracking, prosecuting, and extraditing criminals. Agreements and shared databases between countries can enhance the global response to these crimes.

8. Support for Victims: Establishing support systems for victims of call center crimes can help mitigate the financial and emotional damage. This includes legal assistance, financial counseling, and mental health services to help victims recover and protect themselves from future scams.

By implementing these measures, Thailand can strengthen its defense against call center crimes, protect its citizens, and deter criminals from engaging in these illicit activities.

6. Conclusion

The proliferation of call center crimes represents a multifaceted challenge that transcends national borders and industry sectors, encompassing a range of illegal activities from fraud and scams to identity theft, extortion, money laundering, human trafficking, and unauthorized access to data. This paper has highlighted the complex nature of these crimes, their significant impact on victims and society, and the evolving strategies employed by criminals to exploit technological advancements and regulatory gaps. The legal framework in Thailand, while comprehensive, faces challenges in effectively combating these crimes due to the sophisticated and transnational nature of the operations. The recommendations provided emphasize a holistic approach that includes strengthening regulatory frameworks, enhancing verification processes, developing technological solutions for detection and blocking, and fostering international cooperation and public awareness. By implementing these strategies, it is possible to mitigate the impacts of call center crimes, enhance the resilience of potential victims, and ensure a coordinated response to these threats. The necessity for a multi-pronged strategy that involves legislative reform, technological innovation, and international collaboration is clear. The dynamic nature of call center crimes requires continuous adaptation and vigilance from all stakeholders involved.

As this paper has outlined, the integration of preventive measures, alongside punitive legal actions, forms the cornerstone of an effective response to the challenges posed by call center crimes.

Author Contributions: PK played a pivotal role in the development and execution of this comprehensive review, dedicating efforts across all phases of the project. This included the initial conceptualization, gathering and examining relevant literature, and synthesizing insights to draw meaningful conclusions about call center crimes. PK was responsible for crafting the initial manuscript, incorporating revisions, and refining the narrative to ensure clarity and coherence. As the sole contributor, PK ensured the review's integrity, managing the entire process from ideation to the final compilation, thereby providing a thorough examination of call center crimes, their impacts, and potential countermeasures.

Funding: This paper received no external funding.

Acknowledgments: The authors wish to express their gratitude to the many individuals and organizations that have contributed to the realization of this paper. Special thanks are extended to academic peers for their invaluable feedback, law enforcement, and telecommunications industry professionals for their insights, and the victims of call center crimes who shared their experiences, enhancing our understanding of the issue. This study also benefited from the support of my respective institution, which provided the necessary resources for my paper. My heartfelt appreciation goes to all who played a part in shedding light on the complexities of call center crimes and the ongoing efforts to combat them.

Conflicts of Interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

References

Aksin, Z., Armony, M., & Mehrotra, V. (2007). The modern call center: A multi-disciplinary perspective on operations management research. *Production and operations management, 16*(6), 665-688.

Al-Khater, W., Al-Maadeed, S., Ahmed, A., Sadiq, A., & Khan, M. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access, 8*, 137293-137311. https://doi.org/10.1109/access.2020.3011259.

Anderson, J. (2015). "Tagged as a criminal": Narratives of deportation and return migration in a Mexico City call center. *Latino Studies, 13*(1), 8-27.

Berket, M. R. (2015). Labour exploitation and trafficking for labour exploitation—trends and challenges for policy-making. *ERA Forum, 16*, 359-377.

Brown, G., & Maxwell, G. (2002). Customer Service in UK call centres: Organisational perspectives and employee perceptions. *Journal of Retailing and Consumer Services, 9*(6), 309-316.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*, S47 - S59. https://doi.org/10.1080/14616696.2020.1804973.

Cassim, F. (2015). Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves? *Potchefstroom Electronic Law Journal, 18*, 68-110. https://doi.org/10.4314/PELJ.V18I2.02.

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems, 57*, 245-285.

Colladon, A. F., & Remondi, E. (2021). Using social network analysis to prevent money laundering. *Expert Systems with Applications, 67*, 49-58.

Coverdale, J., Beresin, E., Louie, A., Balon, R., & Roberts, L. (2016). Human trafficking and psychiatric education: A call to action. *Academic Psychiatry, 40*, 119-123. https://doi.org/10.1007/s40596-015-0462-2.

Defossez, D. (2021). Regulations for cybercrimes: The case of the EU Cybersecurity Act. In Handbook of Research on Theory and Practice of Financial Crimes (pp. 453-476). IGI Global.

Deliema, M., Shadel, D., & Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research, 46*(5), 904-914. https://doi.org/10.1093/JCR/UCZ020

De Ruyter, K. O., Wetzels, M., & Feinberg, R. (2001). Role stress in call centers: Its effects on employee performance and satisfaction. *Journal of interactive marketing, 15*(2), 23-35.

Farina, K. A. (2015). Cyber crime: Identity theft. *International Encyclopedia of the Social & Behavioral Sciences, 5*, 633-637. http://dx.doi.org/10.1016/B978-0-08-097086-8.45054-3

Helser, S., & Hwang, M. I. (2021). Identity theft: a review of critical issues. *International Journal of Cyber Research and Education (IJCRE), 3*(1), 65-77. https://doi.org/10.4018/ijcre.2021010107

Holman, D. (2002). Call centres. The new workplace: A guide to the human impact of modern working practices, 115-134.

Hong, B., Connie, T., & Goh, M. K. O. (2023, August). Scam calls detection using machine learning approaches. In 2023 11th International Conference on Information and Communication Technology (ICoICT) (pp. 442-447), IEEE.

Jardine, E. (2015). *Global cyberspace is safer than you Think: Real trends in cybercrime*. Centre for International Governance Innovation and Chatham House. https://doi.org/10.2139/SSRN.2634590.

Jones, C. (2023). That call center tech scammer could be a human trafficking victim. Available at https://www.theregister.com/2023/12/08/human_trafficking_for _cyber_scam/

Kahn, C. M., & Liñares-Zegarra, J. M. (2016). Identity theft and consumer payment choice: Does security really matter? *Journal of Financial Services Research, 50*, 121-159. https://doi.org/10.1007/S10693-015-0218-X

Kale, N., Kochrekar, S., Mote, R., & Dholay, S. (2021, July). Classification of fraud calls by intent analysis of call transcripts. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6), IEEE.

Kempen, A. (2016). Identity fraud-someone stole my identity. *Servamus Community-based Safety and Security Magazine, 109*(12), 36-37.

Keshavarzi, M., & Ghaffary, H. R. (2020). I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review, 36*, 100233. https://doi.org/10.1016/j.cosrev.2020.100233

Kiss, L., Yun, K., Pocock, N., & Zimmerman, C. (2015). Exploitation, violence, and suicide risk among child and adolescent survivors of human trafficking in the Greater Mekong Subregion. *JAMA Pediatrics, 169* 9, e152278. https://doi.org/10.1001/jamapediatrics.2015.2278.

Lewis, J. (2018). Structural Readjustment: Crime, Development, and Repair in the Jamaican Lottery Scam. *Anthropological Quarterly, 91*, 1029 - 1048. https://doi.org/10.1353/ANQ.2018.0048.

Lin, T. C. (2016). The new market manipulation. *Emory LJ, 66*, 1253.

Lohr, S. L. (2019). *Measuring crime: Behind the statistics*. CRC Press.

Malhotra, S., Arora, G., & Bathla, R. (2023, May). Detection and analysis of fraud phone calls using artificial intelligence. In 2023 International Conference on Recent Advances in Electrical, Electronics & Digital Healthcare Technologies (REEDCON) (pp. 592-595). IEEE.

Malkawe, R., Qasaimeh, M., Ghanim, F., & Ababneh, M. (2019). Toward an early assessment for Ransomware attack vulnerabilities. Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems. https://doi.org/10.1145/3368691.3368734.

Mansfield-Devine, S. (2016). Ransomware: taking businesses hostage. *Network Security, 2016*(10), 8-17. https://doi.org/10.1016/S1353-4858(16)30096-4

McMahon, R., Bressler, M., & Bressler, L. (2016). New global cybercrime calls for high tech cyber-cops. *Journal of Legal, Ethical and Regulatory Issues, 19*, 26.

NNT. (2023). Thailand's report of cybercrime crackdown in 2022. Available at https://www.thailand-business-news.com/tech/95761-thailands-report-of-cybercrime-crackdown-in-2022

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks, 7*, 321-327. https://doi.org/10.1049/IET-NET.2017.0207.

Palmer, C., Phillips, D. C., & Sullivan, J. X. (2019). Does emergency financial assistance reduce crime? *Journal of Public Economics, 169*, 34-51. https://doi.org/10.1016/J.JPUBECO.2018.10.012

Park, S., Kim, Y., Yi, S., Lee, S., Na, B., Kim, C., Kim, J., Kim, H., Kim, Y., Park, Y., Huh, I., Kim, H., Yoon, H., Jang, H., Kim, K., Chang, Y., Kim, I., Lee, H., Gwack, J., Kim, S., Kim, M., Kweon, S., Choe, Y., Park, O., Park, Y., & Jeong, E. (2020). Coronavirus disease outbreak in call center, South Korea. *Emerging Infectious Diseases, 26*, 1666 - 1670. https://doi.org/10.3201/eid2608.201274.

Reynolds, L., & McKee, M. (2010). Organised crime and the efforts to combat it: a concern for public health. *Globalization and Health, 6*(1), 1-13.

Robinson, F., & Keithley, J. (2000). The impacts of crime on health and health services: A literature review. *Health, Risk & Society, 2*(3), 253-266.

Sharmeen, S., Ahmed, Y., Huda, S., Koçer, B., & Hassan, M. (2020). Avoiding future digital extortion through robust protection against Ransomware threats using deep learning based adaptive approaches. *IEEE Access, 8*, 24522-24534. https://doi.org/10.1109/ACCESS.2020.2970466.

Siering, M., Clapham, B., Engel, O., & Gomber, P. (2017). A taxonomy of financial market manipulations: establishing trust and market integrity in the financialized economy through automated fraud detection. *Journal of Information Technology, 32*, 251-269. https://doi.org/10.1057/s41265-016-0029-z.

Teichmann, F. (2020). Recent trends in money laundering. *Crime, Law and Social Change, 73*, 237-247.

Weatherburn, A. (2021). *Labour exploitation in human trafficking law*. Intersentia. https://doi.org/10.1017/9781839701559.

Williams, M. J., Bélanger, J. J., Horgan, J., & Evans, W. P. (2019). Experimental effects of a call-center disclaimer regarding confidentiality on callers' willingness to make disclosures related to terrorism. *Terrorism and Political Violence, 31*(6), 1327-1341.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive Intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied, 24*, 196–206. https://doi.org/10.1037/xap0000167.

Zimmerman, C., & Kiss, L. (2017). Human trafficking and exploitation: A global health concern. PLoS medicine, 14(11), e1002437. https://doi.org/10.1371/ journal.pmed.1002437