A Comparative Analysis of the Personal Data Protection Act 2010 in Mitigating Identity Theft and Online Fraud: Malaysia and the United States

Nurul Adli bin Rahmat[1], Nur Khalishah Maisarah binti Mohammad[2], Nur Sarah Afiqah binti Azman[3], Nur Aqila binti Sablihan[4], Lim Jing Xie[5], Koh Huan[6]

[1-5]Universiti Teknologi MARA (UiTM), UiTM Shah Alam

[6]Universiti Kebangsaan Malaysia

DOI: https://doi.org/10.47772/IJRISS.2026.100700514

Received: 24 July 2026; Accepted: 30 July 2026; Published: 06 August 2026

ABSTRACT

This qualitative study compares data protection and identity theft laws in Malaysia and the United States to address escalating online fraud. It evaluates the effectiveness of Malaysia's Personal Data Protection Act (PDPA) 2010 alongside the U.S. Identity Theft and Assumption Deterrence Act 1998. Through document analysis and expert interviews, the research reveals critical structural limitations within the Malaysian framework. The PDPA's applicability is restricted solely to commercial transactions, explicitly excludes government entities, lacks independent prosecutorial authority, and fails to provide direct civil remedies or financial restitution for individual victims. Conversely, the U.S. framework employs a multi-agency, victim-centric approach with mandatory restitution. The study concludes that Malaysia should adopt a hybrid model, incorporating victim-oriented remedies, expanding the scope of data protection, and integrating automated credential filtering to strengthen legal deterrence.

INTRODUCTION

This research explores the legal framework of Malaysia in addressing identity theft and compares it with the existing law in the US. This research will also look at how both countries handle the chosen field of law, enforcement methods, and legal results attained under the existing system. This research also evaluates the implementation, the role of institutions in enforcement, and the efficacy of current remedies or punishments. It uses a critical perspective to identify structural gaps, enforcement constraints, and policy problems that may impede the law's effectiveness in practice. This study also compares the Malaysian with the United States system to highlight Malaysia's strength and shortcomings. This research is significant as it aims to identify the enforcement gaps of PDPA in addressing the issue of identity theft in Malaysia and how US's enforcement model can provide insights to the limitations. Studying these gaps is crucial to understand how Malaysia can strengthen the legal enforcement and evaluate the effectiveness of the current law in regulating the identity theft cases.

Background of study

As per the National Institute of Standards and Technology of U.S Department of Commerce (2019), they define identity theft as terms that are used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data for fraud.[1] Furthermore, in the context of Malaysia, a scam is defined under Section 415 of the Penal Code as any dishonest act of deceit that compels someone to give property or consent to keep property[2]. This involves misleading someone into giving up something valuable or manipulating them into letting someone else retain it.

[1] Newhouse, Johnson et al., Multifactor Authentication for E-Commerce Risk-Based, FIDO Universal Second Factor Implementations for Purchasers Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B) (2019) <https://doi.org/10.6028/NIST.SP.1800-17> accessed in 1 May 2025

[2] Penal Code, s 415.

Online scams due to identity theft were never part of the norm back in the day. According to the Malaysian Computer Emergency Response Team (MyCERT), there were only 3 reported computer fraud incidents in 2000. This was only the beginning, as this number quickly rose to 106 in 2004 and 364 in 2007 which indicates a growing concern for internet user safety while browsing.[3] As years goes by, numerous methods of cybercrime have been invented, including identity theft, which is used for online scams.

Nowadays, it is clear that it has become an uncontrollable issue. CyberSecurity Malaysia reported a 1,192% increase in data theft cases in 2023 compared to 2022, with 646 incidents recorded and these breaches often involved the unauthorized acquisition of Personally Identifiable Information (PII) such as MyKad numbers and banking details, which were subsequently exploited in fraudulent activities.[4] Social media platforms have become fertile grounds for scammers as seen in 2023, the Malaysian Communications and Multimedia Commission (MCMC) received 744 reports of online scams involving Facebook alone and proliferation of scam advertisements and phishing links on this platform has facilitated the mass harvesting of personal data.[5]

The Malaysian Personal Data Protection Act (PDPA) 2010 controls the handling and protection of personal data in the nation. PDPA was enacted on June 2, 2010, in Malaysia and fully came into effect on November 15 2013.[6] It is a thorough legal framework that regulates how personal data is managed, especially in business dealings. PDPA contains seven data protection principles that provide a framework for regulation. These guidelines serve as the basis of PDPA regulations directing organisations towards proper data management procedures. These principles are the General Principle, Notice and Choice Principle, Disclosure principle, Security Principle, Retention Principle, Data Integrity Principle, and Access Principle.[7]

There are no particular provisions about online identity theft in Malaysia's cyber law. Nonetheless, it was proposed that identity theft might be covered by Section 416 of the Penal Code. According to Section 416, it is illegal to cheat by personation which is when someone pretends to be someone else, intentionally replaces someone else or represents themselves or another person as someone they are not. As long as personation occurs, whether it be a real or fictional person, the offence is still committed. However, the Penal Code alone is not enough to address cybercrimes like identity theft. In reality, the Penal Code was undoubtedly not intended to adequately combat cybercrime when it was passed. It is important to remember that this could result in legal loopholes and insufficient cyber protection.

The rapid development of technology has caused new forms of exposure and fraud to all countries, including the United States of America. In 2021, 12% of the total population aged 16 and up were informed that their personal information had suffered a data breach.[8] In 2024, the Federal Trade Commission (FTC) reported 5.7 millions fraud reports and 1.1 million involving identity thefts.[9] The most commonly reported scam was imposter scams where the criminals pretend to be someone they're not or any authority. The total losses to government imposter scams in particular has increased from $171 million in 2023 to $789 million in 2024.[10] Victims are often being

[3] Guan, G. . Phishing: A growing challenge for Internet banking providers in Malaysia. Academia.edu. (2010, August 25) <https://www.academia.edu/308460/Phishing_A_growing_challenge_for_Internet_banking_providers_in_Malaysia?utm_source> accessed in 3 May 2025

[4] Mok, O. CyberSecurity Malaysia reports a steep jump in data thefts last year. Malay Mail.(2024, April 13) <https://www.malaymail.com/news/malaysia/2022/11/23/penang-cops-investigating-claims-of-ic-abuse-during-ge15/41472> accessed in 10 May 2025

[5] Mail, M. MCMC received 744 online scam reports involving Facebook since January. (2023, June 4) <https://www.malaymail.com/news/malaysia/2023/06/04/teo-nie-ching-mcmc-received-744-online-scam-reports-involving-facebook-since-january/72492> accessed in 10 May 2025

[6] Hong, H. Recent Developments in Malaysia's Personal Data Protection Act. (2024, November 14). <https://hhq.com.my/posts/recent-developments-in-malaysias-personal-data-protection-act/> accessed in 13 May 2025

[7] Kiteworks. Everything You Need to Know About the Malaysia Personal Data Protection Act (PDPA) (n.d.). <https://www.kiteworks.com/risk-compliance-glossary/malaysia-personal-data-protection-act/> accessed in 13 May 2025

[8] Harrell, Data breach notifications and identity theft, 2021. (2023, October 2) <https://bjs.ojp.gov/data-breach-notifications-and-identity-theft-2021> accessed in 11 May 2025

[9] Nguyen, S. T, New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024. Federal Trade Comission. (2025, March 10). <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024> accessed in 11 May 2025

[10] FBI, FBI warns public to beware of scammers impersonating FBI agents and other government officials.. (2024, June 5) <https://www.fbi.gov/contact-us/field-offices/portland/news/fbi-warns-public-to-beware-of-scammers-impersonating-fbi-agents-and-other-government-officials> accessed in 11 May 2025

tricked into handing over cash or valuables to fake couriers.

During a financial crisis in 2008 which exposed the serious weaknesses in the U.S consumer financial system, the Consumer Financial Protection Bureau (CFPB) was created to address this issue. Their aim along the way was to protect the consumer and provide themselves with information regarding their rights.[11] Before CFPB, consumer finance laws were enforced by seven distinct agencies, causing confusion in enforcement.[12] Their existence is important in order to be centralized and focused solely on consumer protection in financial services.

Research Problem and Objectives

Identity theft-driven online scams cause severe global losses, exceeding US3.5 billion in losses, while 14% of Australians experienced personal fraud. In Malaysia, 34,497 internet scam cases resulted in RM1.218 billion losses, showing that cybercrime continues to rise and suggesting the Personal Data Protection Act (PDPA) 2010 has not been fully effective in preventing identity theft-related fraud. ISIS Malaysia notes the PDPA still lacks clarity and strength in tackling online scams linked to identity theft, as it does not fully meet international standards due to vague provisions and practical challenges.

To address this, the research objectives are: to examine the effectiveness of Personal Data Protection Act 2010 in Malaysia and Identity Theft and Assumption Deterrence Act 1998 in the United States in addressing online frauds arising from identity theft; to compare the legal frameworks, enforcement mechanisms and policy approaches of both countries; and to propose legal and policy recommendations to strengthen the application of the Personal Data Protection Act 2010 in Malaysia.

RESEARCH METHODOLOGY

This study draws upon primary and secondary data. This research will adopt a qualitative methodology. The primary sources in this study will be the Personal Data Protection Act (PDPA) 2010 and the Identity Theft and Assumption Deterrence Act (ITADA). On the other hand, other secondary sources to be referred to are such as journals, case laws, and reports from the government or non-government, and other online databases such as LexisNexis and Hansard. These informative sources would help in identifying and analysing the history, legislation, usage, and the developments of the PDPA in Malaysia, as well as the cybersecurity protection in the United States. The qualitative data collection for the primary data was generated through semi-structured interviews. Four respondents were selected through purposive sampling.

For this research, semi-structured interviews, either in-person or virtually via Google Meet were. used to collect primary data for this study. This research used purposive sampling, a non-probability sampling technique where participants are chosen based on their relevance to the study’s goals, rather than randomly. Respondents were selected from diverse stakeholders based on their occupational roles and contributions to ensure valuable research outcomes.

LITERATURE REVIEW

Identity theft and Online Fraud

First and foremost, identity theft can be defined as the unlawful theft and abuse of another person's identity, which either benefits the perpetrator or harms the victimThe literature also gives "digital identity theft" as a wide definition for such online crimes. As stated by Mohd Kassim, he contended that the identity theft can be defined using the act itself which is through the use of online channels or identity.

[11] United States Congress, Dodd-Frank Wall Street Reform and Consumer Protection Act, Public Law 111–203, 21 July 2010 <https://www.govinfo.gov/content/pkg/PLAW-111publ203/html/PLAW-111publ203.htm> accessed in 14 May 2025

[12] Consumer Financial Protection Bureau, About Us, Mar. 12, 2025 <https://www.consumerfinance.gov/about-us/the-bureau/> accessed in 14 May 2025

Concept and History of Online Scams

Identity theft has escalated significantly. For instance, 646 incidents recorded and these breaches often involved the unauthorized acquisition of Personally Identifiable Information (PII) such as MyKad numbers and banking details, which were subsequently exploited in fraudulent activities as reported by CyberSecurity Malaysia with a 1,192% increase in data theft cases in 2023 compared to 2022.[13]

The rise of online scams shows the need for mechanism to prevent identity theft from cyber-enabled theft and vulnerabilities in personal data protection. An effective legal framework is needed for effective regulation.

The Malaysian Personal Data Protection Framework

Malaysia enacted the Personal Data Protection Act (PDPA) to strengthen personal data safeguards. This only applied to commercial transaction matters and not in other matters, for example to government agencies and policies. Under **Section 3(1)** of the PDPA 2010, it stated that the government agencies are excluded from being held accountable or in other words, PDPA does not cover or offer legal protection or data leaked from a government department.[14]

Besides we first have to distinguish between personal data and sensitive personal data. Section 4 was revised and amended in 2024, and it strengthened accountability for legal processing by broadening the definition of "sensitive personal data" to encompass biometric data, which means any personal data resulting from technical processing relating to the physical, physiological, or behavioural characteristics of a person as per the same provision.[15] The amendment also includes the definition for 'personal data breach'. A clearer provision in regards to situations such as data breaches, which can be seen in **section 12B** that states that if the data controller believes that a personal data breach has occurred, they shall report and notify the Personal Data Protection Commissioner.[16]

The PDPA 2010 and its amendments in 2024 lays a foundation for legal framework governing collection, processing and protection of personal data in Malaysia, especially in mitigating identity theft risks. Inclusion of biometric data and breach notifications increased public awareness. However, the adequacy in addressing issues of identity theft in an evolving digital environment remains uncertain.

COMPARATIVE ANALYSIS: MALAYSIA AND THE UNITED STATES

The Personal Data Protection Act (PDPA) which regulates personal data processing in commercial transactions is the main legal authority on data breach. It imposes seven core principles that data users need to comply with in collecting, processing and storing data. Lilynn (2017) notes that the regulatory framework of the PDPA has been strengthened through the introduction of the PDPA Standard 2015 and the Personal Data Protection (Class of Data Users) (Amendment) Order 2016.[17] While the PDPA supports Malaysia's digital economy and aligns with international data protection standards, it does not address criminalization of identity theft. As noted by Yoon et al. (2019), the Act primarily addresses harms arising from the disclosure or misuse of personal data by imposing duties on data users, rather than providing direct remedies for victims of identity theft.

The surge digitization of personal transactions and the widespread use of online platforms has evolved as a critical concern of identity theft in Malaysia.[18] Under Malaysian cyber law, identity theft is instead addressed under Section 416 of the Penal Code, which criminalises “cheating by personation,” may apply where an offender

[13] Mok, O. CyberSecurity Malaysia reports a steep jump in data thefts last year. Malay Mail.(2024, April 13) <https://www.malaymail.com/news/malaysia/2022/11/23/penang-cops-investigating-claims-of-ic-abuse-during-ge15/41472> accessed in 10 May 2025

[14] Section 3(1), Personal Data Protection Act 2010 (Act 709).

[15] Personal Data Protection (Amendment) Act 2024, s 4.

[16] Personal Data Protection (Amendment) Act 2024, s 12B.

[17] Noor Sureani, N. B., Awis Qurni, A. S. B., Azman, A. H. B., Othman, M. B. B., & Zahari, H. S. B. The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. Malaysian Journal of Social Sciences and Humanities (MJSSH), 6(10), 488–495. (2021). <https://doi.org/10.47405/mjssh.v6i10.1087> accessed 27 December 2025

[18] Ibid.

impersonates another person, substitutes one person for another, or falsely represents an identity and is punishable under Section 419 with imprisonment of up to seven years and/or a fine.[19] However, while these provisions may apply where identity impersonation happens, reliance on the Penal Code is inadequate as it was enacted in a pre–information technology era and was not designed to address cybercrime. Additionally, the Computer Crimes Act 1997 and the Communications and Multimedia Act 1998 may also be invoked where unauthorized use of computers or fraudulent use of network facilities are involved.[20]

In contrast to Malaysia's approach, the United States (US) recognises identity theft as a federal offence. The Identity Theft and Deterrence Act 1998 acknowledge identity theft as a crime when someone commits an intentionally transfers or misuses another individual's identification without legal permission for the purpose of committing or aiding a felony.[21] The United States defines identity theft as unauthorized transfer, acquisition or use of another person's personal or financial information for personal gain.[22] Prior to its enactment, identity theft was neither expressly regulated nor investigated as a distinct offence.[23] Law enforcement relied on limited federal statutes protecting specific information and on general anti-fraud laws to address resulting harm. Rapid increase in identity theft prompted legislative intervention to address this issue. The Act serves two main objectives, to criminalise identity theft at federal level and provide victims with a right to restitution. Following this enactment, most U.S states enacted their own identity theft statues. By 2023, all fifty states had enacted identity theft legislation providing restitution for victims yet identity theft continued to increase alongside technological advancement.

Identity Theft and Deterrence Act 1998 is first federal law to criminalise identity theft, establishing penalties for both completed and attempted offences and allowing for the forfeiture of property used or intended for use in the fraudulent activity. Overall, the above comparison shows that both countries have different regulatory philosophies in addressing identity theft and protecting personal data where Malaysia focuses on preventive data governance while the U.S. adopts a crime-centered approach.

Enforcement Mechanism

The Governance of the Data Protection

Malaysia and the United States both recognise the importance of protecting personal data but they adopt fundamentally different ways to enforce their data protection laws. Malaysia's enforcement framework prioritises administrative and compliance, while the United States prioritises criminalisation and multi-agency enforcement.

Malaysia

In Malaysia the main authority that is responsible for enforcing data protection law is the Personal Data Protection Commissioner (PDPC).[24] It was created under the Ministry of Digital on 15 November 2013 and acts as Malaysia's independent data protection authority which is responsible for overseeing the implementation and enforcement of the PDPA 2010.[25] The PDP Commissioner is responsible for regulating the process of commercial transactions of personal data by organizations (Data Controllers) and protecting the interests of individuals from any misuse of personal data.[26] However, the PDPA role is only supervisory because it does not operate as a law enforcement agency and does not possess policing powers such as arrest, seizure of assets, or criminal

[19] Identity Theft. Richard Wee Chambers. (2020, September 3). <https://www.richardweechambers.com/identity-theft/> accessed 27 December 2025
[20]Ibid
[21]Identity theft investigations | EBSCO. (2024). EBSCO Information Services, Inc. | Www.ebsco.com. <https://www.ebsco.com/research-starters/law/identity-theft-investigations> accessed 27 December 2025
[22] Ibid
[23] Identity Theft and Assumption Deterrence Act of 1998. The IT Law Wiki; Fandom, Inc. <https://itlaw.fandom.com/wiki/Identity_Theft_and_Assumption_Deterrence_Act_of_1998 (2025)> accessed 27 december 2025
[24] Department of Personal Data Protection (JPDP), 'Department Profile' (Official Portal, 2024) <https://www.pdp.gov.my/ppdpv1/en/mengenai-jpdp/profil-jabatan/> accessed in 31 December 2025.
[25] Ibid et 23, s 47.
[26] Sonny Zulhuda, 'The Personal Data Protection Act 2010: A Leap Forward or a Half-Step?' [2011] 4 Malayan Law Journal i.

interrogation.[27] Overall, Malaysia's centralised administrative model emphasizes regulatory preventive measures and supervisory rather than actively pursuing criminals who misuse stolen personal data. [28]

The Malaysian Communications and Multimedia Communication act as a support to assist the PDPC in cases involving online scams and digital platforms, especially where identity theft happens through telecommunications networks or social media.[29] However, MCMC operates under separate legislation, and coordination between agencies often has flaws.[30] This style of governance structure can delay enforcement responses, especially in complex cybercrime cases.[31] That said, major structures produce major weaknesses in Malaysia's system in the area of the exclusion of government agencies from the scope of PDPA which means that personal data handled by public sector bodies is not subject to the same regulatory standards or enforcement mechanisms which can create a significant accountability gap and weaken overall data protection governance. [32]

The United States

In contrast with Malaysia's governance, in the United States (US), they adopt a multi-agency enforcement model rather than a single overarching authority.[33,34] Instead, governance is distributed among several agencies with complementary mandates.[35] The Federal Trade Commission (FTC) functions as the main civil regulator for data protection, consumer privacy and also identity theft where they oversee corporate data practices and can take civil action against companies that fail to implement reasonable security measures under **Section 5 of the FTC Act**.[36] They are led by the agencies such as the Federal Bureau of Investigation (FBI) and also the Department of Justice (DOJ) which is responsible for investigating and prosecuting identity theft as a federal crime.[37]

This parallel enforcement framework allows regulatory enforcement and criminal justice enforcement to operate simultaneously.[38] Corporate negligence and criminal misconduct are treated differently but addressed within the same enforcement ecosystem.[39] As a result, identity theft is not viewed merely as a compliance issue, but as a serious threat to public trust and economic security.[40] Unlike Malaysia's supervisory model, the US emphasizes on criminal accountability and public protection.

Investigation Powers of Search and Seize Authority

Under Sections 101 to 103 of the PDPA 2010, the Personal Data Protection Commissioner has investigatory powers, including authority to enter premises, inspect documents, and also access computerised data.[41] These powers are generally administrative in nature and are mainly focused on compliance, not punishing criminal conduct.[42] While this way of approach aligns with regulatory best practices in fostering compliance, it is less effective in responding to identity theft, which is inherently criminal and often involves intentional wrongdoing.[43]

[27] Jillian Chia and Nicole Oh, 'Data Protection & Privacy 2020' (Skrine, 1 January 2020) <https://www.skrine.com/insights/publications/2020/january/data-protection-privacy-2020> accessed 31 December 2025.
[28] Ibid
[29] Communications and Multimedia Act 1998 (Act 588), s 263.
[30] Rahmah Ismail, 'Legal Protection of Consumers against Online Scams in Malaysia' (2020) 24(1) Journal of Information and Communication Technology Law 45.
[31] Ibid.
[32] Personal Data Protection Act 2010 (Act 709), s 3(1).
[33] Federal Trade Commission, 'Privacy and Security Enforcement' (Official Website, 2025) <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 31 December 2025.
[34] Congressional Research Service, 'Data Protection Law: An Overview' (R45631, 2019).
[35] Ibid.
[36] Federal Trade Commission Act, 15 USC § 45.
[37] Identity Theft and Assumption Deterrence Act 1998, 18 USC § 1028; see also US Department of Justice, 'Identity Theft' (Criminal Division, 2023) <https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> accessed 31 December 2025.
[38] Federal Bureau of Investigation, 'White-Collar Crime' (Official Website, 2025) <https://www.fbi.gov/investigate/white-collar-crime> accessed 31 December 2025.
[39] Ibid.
[40] Identity Theft Penalty Enhancement Act 2004, Pub L No 108-275, 118 Stat 831.
[41] Personal Data Protection Act 2010 (Act 709), s 101-103.
[42] Ibid.
[43] Abu Bakar Munir and Siti Hajar Mohd Yasin, Personal Data Protection in Malaysia: Law and Practice (Sweet & Maxwell Asia

The Commissioner cannot conduct criminal investigations, thereby limiting the depth and urgency of investigations involving sophisticated cybercriminals.[44]

The US investigates identity theft through criminal procedure, like search warrants, forensic digital analysis and financial tracing to identify offenders and recover losses.[45] The emphasis is on building prosecutable cases. This enables a swift escalation from a detection to prosecution, particularly in cases involving large-scale identity theft, data breaches, or interstate criminal syndicates.[46] From the above comparison, it shows that while Malaysia's approach supports compliance, the US criminal approach provides stronger deterrence and faster response to offender conducts.

Prosecutorial Process

Malaysia's prosecutorial process of enforcement framework is the critical weakness that needs to be addressed. Under Section 124 of the PDPA 2010, it expressly requires the written consent of the Public Prosecutor before any prosecution may be initiated.[47] Despite being the main enforcement authority, the Personal Data Protection Commissioner lacks independent prosecutorial standing.[48] These multi-layered approvals are time consuming as they create delays and may discourage any aggressive enforcement, especially where cases involving technical breaches rather than a clear criminal intent.[49] As a result, most breaches are resolved administratively.[50]

Meanwhile, the United States prosecution process allows the federal prosecutors to initiate proceedings directly through the Grand Jury system.[51] Identity theft offences under 18 U.S.C § 1028 and § 1028A are classified as felonies. enabling rapid escalation from investigation to indictment.[52] This process of direct prosecutorial authority enhances deterrence and signals the seriousness with which identity theft is treated within the criminal justice system.[53] This shows that the US process allows quick, offender-focused action while Malaysia's reliance on administrative enforcement slows response and reduces deterrence.

The PDPA's amendments provides for fines up to RM1,000,000[54] and custodial sentences of up to three years, but imprisonment is rarely imposed, especially for corporate data breaches.[55] They target breaches of handling data more than identity theft itself.[56] This limitation is evident in Section 2 of the PDPA, which restricts the Act's application to commercial data processing, leaving unauthorised use of data and identity theft out of its direct reach.[57] Malaysia's economic and administrative sanctions offer limited deterrent effects.

The United States, however, adopts a markedly punitive approach.[58] Under § 18 U.S.C. § 1028A, aggravated identity theft carries a mandatory minimum sentence of two years' imprisonment and to be served consecutively.[59] The United States further strengthened enforcement through Identity Theft Enforcement and

2010).

[44] Ibid note

[45] US Department of Justice, 'Identity Theft' (Criminal Division, 2023) <https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud> accessed 31 December 2025.

[46] Federal Bureau of Investigation, 'Cyber Crime' (Official Website, 2025) <https://www.fbi.gov/investigate/cyber> accessed 31 December 2025.

[47] Personal Data Protection Act 2010 (Act 709), s 124.

[48] Ibid

[49] Ibid.

[50] Ibid..

[51] US Constitution, amend V

[52] Identity Theft and Assumption Deterrence Act 1998, 18 USC § 1028; Identity Theft Penalty Enhancement Act 2004, 18 USC § 1028A.

[53] Ibid .

[54] Personal Data Protection (Amendment) Act 2024, s 5 (amending s 5 of Act 709).

[55] Ibid.

[56] Abu Bakar Munir and Siti Hajar Mohd Yasin, Personal Data Protection in Malaysia: Law and Practice (Sweet & Maxwell Asia 2010).

[57] Personal Data Protection Act 2010 (Act 709), s 2(1).

[58] US Sentencing Commission, 'Quick Facts on Section 1028A, Aggravated Identity Theft Offenses' (2024) https://www.ussc.gov/research/quick-facts/aggravated-identity-theft accessed 31 December 2025.

[59] Ibid at 46, 18 USC § 1028A.

Restitution Act 2008 (ITERA).[60] Under 18 U.S.C. § 3663(b)(6), the courts are empowered to order restitution for victims. This ensures punishing offenders and recognizes harms caused to the victims. [61] The different approaches Malaysia and the US take reflect differences in deterrence and victim protection.

Remedies

Under the Malaysian PDPA, individuals may file complaints with the Personal Data Protection Commissioner but the remedies available under the PDPA itself are limited.[62] If breach is proven, the commissioner may issue enforcement notices or impose fines on the organisations involved. However, these fines will be going to be paid to the government, not the victims.[63] Individuals affected receive no compensation from the fines.[64] Victims seeking restitution must proceed with separate civil claims which can be both time and cost consuming.[65] This discourages many from taking legal action.[66]

In contrast, the United States places greater emphasis on helping victims recover from identity theft.[67] In most cases, the court can order offenders to repay victims for losses caused by identity theft.[68] Restitution in the United States is not limited to direct financial loss. It may include costs related to fixing credit records, legal fees, and time spent to resolve issues on identity theft.[69] This highlights that the law recognises the real and ongoing impact of identity theft on victims' lives.[70] The Federal Trade Commission operates an identity theft reporting system that helps victims document their cases, report fraud, and take steps to restore their identity. This is able to reduce the burden on victims and makes the recovery process controllable.[71] By combining criminal punishment with victim compensation, the U.S. framework ensures that enforcement benefits both states and victims. [72]

In conclusion, while Malaysian remedies are largely regulatory and indirect, US remedies are punitive and victim-centered, giving a more comprehensive protection and compensation. **3.3 Effectiveness in Addressing Identity Theft and Online Fraud**

Malaysia's Personal Data Protection Act (PDPA) has several structural limitations that weaken its effectiveness. Unlike data protection regimes such as the GDPR, the PDPA does not impose revenue-based fines linked to a company's annual global turnover reflecting a comparatively lower level of data security enforcement.[73] In terms of remedies, Mohamed and Zulhuda (2019) note that individuals affected by PDPA breaches cannot initiate statutory civil actions against data users as the Act does not provide for civil liability instead victims must rely on common law or tort claims for invasion of privacy arising from data misuse.[74] Additionally, the PDPA's application is restricted to commercial transactions excluding personal data collected through social media platforms such as Facebook, Twitter and Instagram. This regulatory gap has contributed to large-scale data leaks, including the exposure of personal information of over 11 million Malaysian Facebook users (Chapree, 2021).[75] The PDPA further excludes federal and state governments from its scope by granting public authorities broad discretion over personal data protection. As Yaakob (2016) argues, this exclusion undermines privacy safeguards particularly given that government agencies such as the National Registration Department store highly sensitive

60 Identity Theft Enforcement and Restitution Act 2008, Pub L No 110-326, 122 Stat 3560.
61 Ibid.
62 Personal Data Protection Act 2010 (Act 709), s 2.
63 Ibid.
64 Ibid.
65 Azmi & Associates, 'Criminal and Civil Liability of Data Breaches under the Malaysian Law' (Official Website,2025) <https://www.azmilaw.com/insights/criminal-and-civil-liability-of-data-breaches-under-the-malaysian-law/> accessed 31 December 2025.
66 Ibid.
67 Identity Theft Enforcement and Restitution Act 2008, Pub L No 110-326, 122 Stat 3560.
68 Ibid.
69 Ibid.
70 Ibid.
71 Federal Trade Commission, 'IdentityTheft.gov' (Official Website, 2025) <https://www.identitytheft.gov/> accessed 31 December 2025
72 Identity Theft Enforcement and Restitution Act 2008 (n 12).
73 Ibid.
74 Ibid.
75 Ibid.

personal and financial data.[76] Exempting the largest data holders in Malaysia from PDPA compliance ultimately diminishes the Act's purpose and effectiveness in protecting personal data.

The adequacy of law in identity theft in the U.S. also has been a debate. Despite the existence of federal identity theft offences, enforcement remains uneven in practice. Although federal criminal law imposes penalties of up to twenty years' imprisonment on individuals who knowingly produce, use or traffic in false identification devices with intent to defraud, many identity-related offences involve relatively small financial losses and are therefore often deprioritised due to limited investigative and prosecutorial resources.[77] Civil remedies are also inadequate as common law does not recognise personal identity itself as a protected personal or property interest. While physical identification documents such as credit cards and driver's licences constitute personal property, they merely represent identity rather than embody it.[78] Consequently, courts have not classified identity as tangible personal property. Moreover, the tort of fraud which requires a misrepresentation made to induce reliance offers little relief to identity theft victims as it does not directly address the unauthorised misuse of one's identity.[79]

In the case of **WT Development Sdn Bhd v Chow Cho Tai & Ors**[80], the High Court of Kuala Lumpur addressed a significant instance of identity theft and corporate fraud where the victim, Mdm. Chow Cho Tai discovered her personal particulars and forged signatures were used without her knowledge to facilitate an unlawful property transfer. The defendants including directors of the insolvent company Rimau Indah used Mdm. Chow's identity to falsely name her as a director and trustee in order to transfer a valuable piece of property to a shell company, Jiwa Rakyat, effectively shielding the asset from liquidators and creditors. The fraud was only discovered when the company's liquidators threatened Mdm. Chow was charged with criminal prosecution for failing to provide the company's financial statements, leading her to conduct a company search and file police reports.

The court's doctrinal analysis of the identity theft emphasized the severe injury caused to the victim even in the absence of a standalone identity theft statute in Malaysia. Because her identity was used to facilitate a land sale that eventually yielded over RM8 million for the conspirators, the court remarkably noted that her identity was "worth more than RM8 million" to the perpetrators. Mdm. Chow successfully proved that the defendants had committed abuse of process while the law firm involved was found liable for negligence after a handwriting expert and immigration records proved she was in Australia when she was purportedly "signing" documents in Malaysia. Ultimately, the court awarded substantial general, aggravated and exemplary damages to compensate for her psychological distress, legal expenses and the grave threat of criminal conviction she faced due to the theft of her identity.

The unfortunate nature of identity theft can be further illustrated by the case of **Rogan v City of Los Angeles**[81] whereby the severe consequences of identity theft compounded by inaccurate electronic records. In 1981, an escaped prisoner, McKandes assumed Terry Rogan's identity after obtaining his birth certificate and used it to acquire identification documents in California. While using Rogan's identity, McKandes was arrested in 1982 and later became the subject of an arrest warrant issued in Rogan's name for two robbery-murders. This warrant was entered into the National Crime Information Center (NCIC) database making it accessible nationwide along with McKandes' physical characteristics and fingerprints.

Between 1982 and 1984, Rogan was repeatedly arrested and detained across several states following routine police checks that relied on inaccurate NCIC data despite fingerprint comparisons confirming that he was not the suspect. Although the record was temporarily removed, the Los Angeles Police Department (LAPD) re-entered the erroneous information multiple times which then led to further wrongful arrests involving drawn weapons, handcuffing, detention and imprisonment. Rogan subsequently sued the City of Los Angeles under 42 U.S.C. § 1983 for violations of his constitutional rights. The court held that the LAPD's handling of the NCIC database

[76] Ibid.

[77] Saunders, K. M., & Zucker, B. Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act. International Review of Law, Computers & Technology, 13(2), 183–192. (1999). <https://doi.org/10.1080/13600869955134> accessed 31 december 2025

[78] Ibid.

[79] Ibid.

[80] WT Development Sdn Bhd v Chow Cho Tai & Ors [2019] MLJU 1691

[81] Rogan v City of Los Angeles 668 F. Supp. 1384 (C.D. Cal. 1987)

was grossly negligent and awarded judgment in Rogan's favour for the pain and humiliation he suffered due to the mistaken arrests.

Comparative Evaluation and Best Practice

This section compares and evaluates the Personal Data Protection Act 2010 (PDPA) and the Identity Theft and Assumption Deterrence Act 1998 (ITADA) by examining how each legal framework balances rights and enforcement effectiveness in addressing identity theft and online fraud.

. As previously mentioned, despite the **Personal Data Protection Act (PDPA) 2010** regulating the collection, use, and disclosure of personal data and imposing criminal penalties on data users who violate its provisions, its criminal offences are mostly restricted to violations of data processing obligations.[82] For example, data users who handle personal data without authorisation, violate data protection principles, or unlawfully disclose or sell personal data are subject to penalties and/or imprisonment under **Section 131 of PDPA**[83]. On the other hand, the unauthorised possession, use, or transfer of another person's personal identification with the intent to commit fraud or other crimes outside of the regulated data processing context is not criminalised by these provision as seen in **Section 2 of PDPA** whereby it emphasizes that the act applies to any personal data in respect of commercial transactions which show that non-commercial fraud falls outside the scope[84]. Not to mention, as per **Section 5 of PDPA,** it merely serves as a function where fines are paid to the government, which leaves the victim with the burden of remediation[85].

Meanwhile, the **Identity Theft and Assumption Deterrence Act (ITADA**) of the United States, which is codified in **18 U.S.C. § 1028,** expressly forbids trafficking in authentication features that are used to create false identification and makes it illegal to use another person's "means of identification" with the intent to commit or facilitate unlawful activity[86]. Furthermore, the **Identity Theft Enforcement and Restitution Act of 2008 (ITERA)**, as stated in 1**8 U.S.C. § 3663(b)(6)**, provides another jurisdiction in the United States for identity theft cases, which may include restitution orders equal to the value of the victim's time spent remediating the actual or intended harm of identity theft or aggravated identity theft.[87] Thus, while ITADA provides the foundational rationale for criminalization, ITERA ensures that the law addresses the substantive burden placed on the individual victim[88].

That being said, by adopting a similar approach, Malaysia might strengthen its data security framework by establishing a distinct identity theft offence that focuses on the unauthorised use or disclosure of personal identifiers such as passports or identification card numbers. This would provide a strong criminal deterrent in addition to the regulatory focus of the PDPA. Such reform would protect people from modern identity theft, improve privacy rights, close the existing legal gap, and increase public confidence in online and offline identity security. To illustrate, Malaysia can embrace a hybrid model that aligns with the US's "victim-centric" approach to data autonomy by keeping the PDPA's regulatory penalty but adding a restitution clause for victims.

In conclusion, the legal systems of Malaysia and the US have been examined in this chapter, with an emphasis on how each country protects personal data in a world economy that is becoming more and more digital. A comparison of the Identity Theft and Assumption Deterrence Act (ITADA) with the Personal Data Protection Act (PDPA) 2010 reveals many differences in enforcement strategies and policy approach in regard to identity theft and also the effectiveness in addressing the said problem. This analysis highlights two primary shortcomings in Malaysia which that the law's restriction to "commercial transactions" and its inability to compensate victims for wasted time and effort. Overall, Malaysia lacks the "victim centric" which is evident used in the US frameworks. Accordingly, Malaysia should take into account a hybrid legal approach in order to proceed that would create a new criminal statute expressly for identity theft in addition to the business laws of the PDPA.

82 Ibid.
83 Personal Data Protection Act 2010 (Act 709), s 131.
84 Personal Data Protection Act 2010 (Act 709), s 2.
85 Personal Data Protection Act 2010 (Act 709), s 5.
86 Ibid.
87 Identity Theft Enforcement and Restitution Act of 2008, 18 U.S.C. § 3663(b)(6)
88 Office for Victims of Crime (OVC).Expanding Services To Reach Victims of Identity Theft and Financial Fraud - Federal Identity Theft Laws. (2010) <https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/pfv.html> accessed in 23 December 2025

Incorporating a restitution mechanism requiring offenders to reimburse victims for the time spent correcting their identification in the digital era, Malaysia can strengthen public trust and improve citizen protection.

ANALYSIS AND FINDINGS

This analysis demonstrates that identity theft in Malaysia constitutes a serious and escalating problem that remains inadequately addressed. All respondents agree that the shift from traditional paper-based transactions to online platforms is a key contributing factor to the rise of identity theft. They recognize that a significant amount of personal data is now residing in the public domain which makes it easier for identity theft to access sensitive information.

Seriousness and Causes of Identity Theft

Respondent 1 emphasized that the communications technology has moved so much faster than the law[89]. They argue that the traditional legal framework is no longer adequately aligned with realities of cybercrime because the PDPA was formulated in 2010. They stated that the law must be developed as technology is evolving. This respondent viewed the cause as a structural failure of the state to keep the law in line with technological activity. Their focus is on the jurisdictional mismatch between the global digital trends and also local legal applications. Furthermore, respondent 1 also highlights that while Malaysia looks at international legal models, they warn that foreign laws may not suit Malaysia's own culture and backgrounds. This shows that a general law copying from jurisdiction outside Malaysia may lead to poor enforcement and relevance to the local.

Respondent 2 categorized the cause into two distinct parts which are the first part is the data people put out voluntarily via social media or LinkedIn and the second part is the data leaked out via breached without consent.[90] This respondent placed more emphasis on individual behavior and corporate accountability. They highlighted that even the professional platforms can be a source of risk if the personal data is being over shared. Respondent 2 focused on practical consequences of theft, which is someone assuming an identity to apply for services such as employment or bank loans. From the perspective of the respondent, the seriousness is tied to the long-term damage that an individual faces when their legal persona is used for financial or professional services.

Awareness and Effectiveness of PDPA

In Malaysia, the Personal Data Protection Act (PDPA) 2010 was enacted to regulate the processing of personal data in commercial transactions and to safeguard the individuals against the misuse of their personal information. Based on the interview, respondents generally acknowledged the purpose and importance of the PDPA. However, they agree that its effectiveness is limited, particularly in the modern context of modern online scams.

Respondent 1 emphasized that the PDPA was enacted in 2010 where the technology usage is limited and digital transactions were usually conducted in a traditional method which is by in-person[91]. The online platforms like digital banking are also not commonly used during this time period which make the legislative framework outdated in understanding how personal data is collected, processed and exploited nowadays. She also highlights that there are gaps in the PDPA's ability in addressing the current methods of identity theft such as malware attacks and online scams as these modern threats were not fully anticipated when the law was enacted. Consequently, the protection provided in PDPA is not sufficiently effective in preventing latest technological risks. Additionally, she also addressed that the enforcement by agencies also weakened the Act's effectiveness due to manpower shortages in the agencies, cross-agency coordination issues, frequent transfer of officers between departments and outdated training modules. While in terms of awareness, the respondent highlighted that the increased digital users does not correspond to a sufficient public understanding of data security risks or the extent of personal data being protected. Individuals are often required to provide personal information online to access government benefits or services but with little explanation regarding the data safety and no alternative options.

89 *Ibid* at p 55.
90 *Ibid* at p 55.
91 *Ibid* at p 55.

Respondent 2 adopted a more balanced perspective where Malaysia's data protection framework was legally robust in principle[92]. The PDPA has strong provisions that govern data breaches and security failures and is supported by other legislation such as the Computer Crimes Act. However, the law is only words on paper and it cannot deter criminal behaviour without proactive enforcement by regulators and responsible data protections safeguard by private entities. She also believed that the data subject themselves must also have a strong sense of awareness on data protection in order for the law enforcement to be effective. The respondent further emphasized that data subjects themselves must have control over personal data for the law to operate effectively. This means PDPA also requires enforcement and public engagement to be effective.

Respondent 3 also supported the view that PDPA only provides limited protection against identity theft.[93] Despite being familiar with the PDP since its drafting, the respondent observed that the law is more effective in governing the companies in handling the data than in directly combating this issue. Measurements such as data retention policies and security principles were acknowledged by him to be beneficial as they reduce the risk of personal data being exposed. Nevertheless, he noted that most identity theft cases arise from social engineering techniques which are outside the scope of PDPA. Additionally, the respondent highlighted that PDPA enforcement authority has limited powers and tends to focus on procedural breaches rather than complex scam offences, further limiting the Act's effectiveness in addressing identity theft.

Sufficiency of PDPA and Current Legal Framework

Respondent 1 questioned the adequacy of the PDPA, describing it as outdated and inadequate to combat identity theft. Even though there was an amendment that has been done to the act, it is minor and does not have a significant impact on addressing the new emerging issues relating to identity theft.[94] The respondent also noted the insufficiency by section 3 exemption of the PDPA that states the PDPA does not apply to the Federal and State governments despite the amendments. Since the government holds most of our data through system and mandatory registration such as MyDigital ID which allows our data to risk being stolen. Using the WISE case as illustration, Respondent 1 highlights identity theft is also a risk in cross-border data transactions.

Respondent 2 has a more positive view of the PDPA, stating that it alights with the GDPR.[95] They pointed to the seven core data protection principles which include disclosure, consent and security which have imposed robust obligations on private entities. A key highlight is the 2025 mandatory data breach notification requirement that is an important critical safeguard by informing all regulators. While the respondent mentioned that law cannot physically prevent crime, the PDPA provides a comprehensive framework for enforcement. Overall, Respondent 2 views the current framework as powerful enough to cater this issue.

Meanwhile, Respondent 3 argues that the PDPA alone is insufficient and requires supplementary legislation. Respondent 3 referred to recent laws like Online Safety Act 2025 and Cyber Security Act 2024 which mandates licensing for online platforms to combat financial fraud and secures critical data.[96] Respondent 3 critiques the lack of clear remedies for victims where they pointed out the backlog in financial dispute channels and the ambiguity on the matter of whether the banks or platforms should be liable for identity theft despites the developments. Additionally, delays in dispute resolution mechanisms and unresolved jurisdictional issues were identified as ongoing weaknesses within the current legal framework.

Enforcement Challenges

A key challenge identified by Respondent 1 is jurisdictional ambiguity arising from the cross-agency enforcement. PDPA enforcement requires cooperation by various agencies including the Personal Data Protection Commissioner (PDPC), the Malaysian Communications and Multimedia Commission (MCMC), the policy and other regulatory bodies.[97] PDPA only spelled out the authority for PDPC in addressing this issue but was silent

92 *Ibid* at p 55.
93 *Ibid* at p 55.
94 *Ibid* at p 55.
95 *Ibid* at p 55.
96 *Ibid* at p 55.
97 *Ibid* at p 55.

on some enforcement mechanisms, specifically on immediate administrative actions. While the PDPA confers authority on the PDPC, lacking clear provisions on administrative powers results in reliance on crime investigation by the police. Respondent 2 also shares the same concern.[98] The reliance on external bodies subsequently led to lengthy enforcement processes and weakened the practicality of the PDPA. Respondent 1 added that outdated nature of PDPA is the cause of the jurisdictional ambiguity. Relying on external enforcement mechanisms delays and weakens the PDPA in responding to identity theft.

Respondent 3 further notes that the limited enforcement powers of the PDPA results in selective enforcement practices, where authorities tend to focus on non-compliance of procedure rather than prosecution.[99] Similarly, he also identified significant legislative gaps within the PDPA in which there is an absence of a right to initiate civil proceedings and non-applicability to the government which causes the individuals to not obtain any remedies in cases involving government and overseas data breaches.

Further enforcement challenges arise from limited manpowers and budget which is underlined by Respondent 2 and Respondent 3. Both respondents mentioned the limitations of budgets and manpowers making it impractical to investigate every single data breach case and complaint. Hence, the majority of the cases were left hanging and many individuals' complaints remain unresolved as the enforcement becomes more selective in handling the cases and frequently prioritises cases with a larger public impact. Although it is necessary for the authorities to be selective in order to ensure efficiency, it indirectly reduces public confidence in the enforcement.

Comparative Insights & Lessons for Malaysia

Respondent 1 bring out that US government have a system that has automatic notifications to inform the users of any platforms if there were any attempted action to use their identity that they have submitted for any transactions pertaining to the deals they made which made a comparison in Malaysia, the notification for the users to alert the action does not apply in the country.[100] Respondent 1 believes that this automated notification shall be a good practice to also apply in Malaysia for users that submitted their personal information online.

Respondent 3 added that Malaysia adopts more laws by referring to EU data protection laws which brings the GDPR that most EU countries use and may adopt some of the laws from the US.[101] The respondent also highlights that Malaysia will refer to data protection in the EU rather than US. The US has a legal framework for identity theft which is Identity Theft Assumption Deterrence Act 1988 (ITADA) while Malaysia has Personal Data Protection Act 2010 (PDPA). One key difference is where the US has a multi-layered federal state enforcement environment while Malaysia operates in a centralised federal regulatory framework. Respondent 1 opined that Malaysia has a very dominant federal government which would not be suitable to adopt US laws. Respondent 1 also proposed that Malaysia may adopt a credit reporting and credential filtering system similar to the US to check consumer credentials before approving loans and transactions. While the US Identity Theft Assumption Deterrence Act (ITADA) provides a robust model for combating identity theft, its dual federal-state structure is fundamentally incompatible with Malaysia's centralized federal system. Therefore, the respondents agreed not to copy the US legislative structure but to adopt its functional tools. Specifically, integrating US-style credit reporting and credential filtering systems could provide the enforcement that the current PDPA lacks in preventing financial fraud before it occurs.

Respondent 1 suggests the credit filtering system by the US can be a guidance and adopt the system in Malaysia. The automatic notifications to alert the users of online platforms can be installed on the devices that can be applied across the platforms if there were any attempts of identity theft to detect for a swift action to be taken care of. Respondent 1 also highlights that the PDPA can be reformed however it must take into consideration by interviewing other stakeholders that are usually involved with these matters to scrutinise the challenges on how PDPA can be improved.

Respondent 2 assert Malaysia data protection does not have much that is lacking but the respondent believe PDPA

98 *Ibid* at p 55.
99 *Ibid* at p 55.
100 *Ibid* at p 55.
101 *Ibid* at p 55.

does not apply to federal and state government is the gap that need to be improved although most of the information undeniably the government have the citizen's personal data. Respondent 2 also said that most recent cases of breach of identity were from the government databases which prove that the government does not have the accountability to be responsible towards these data breaches. In addition, the respondent said it is crucial to have public awareness as a lot of entities like companies collect too much personal information that most likely the data can be leaked. It is vital that the people must know where and to whom they give the personal information. Moreover, the data given shall be minimised which is the key to avoid the cases of identity theft.

CONCLUSION

The Personal Data Protection Commissioner (PDPC) is the primary authority in enforcing data protection law. The PDPA sets out the function and powers of the commissioner in addressing data protection issues. The commissioner has express authority in regulating the administrative structure of data processing in commercial transactions and protecting the interests of individuals from any data misuse. However, their responsibility role remains supervisory with limited authority in enforcement. The commissioner's jurisdiction should be expanded to include stronger enforcement powers.

Additionally, the investigating and punishment powers of the PDPA should be expanded. The current legal framework requires the data breach and identity theft cases to be initiated through court proceedings and go through a lengthy criminal procedure. This procedure leads to delay and disrupts the enforcement process as the number of cases continue to increase. By granting PDPA's power to impose penalties and conduct investigations, this would strengthen enforcement capacity and reduce reliance on external authorities and directly affect the number of cases to be responded swiftly.[102] Hence, enhancing the PDPC's investigative and punitive powers would ensure the cases are addressed systematically and efficiently.

The improvement of coordination between regulators and law enforcement agencies is also essential. Data protection enforcement frequently overlaps with general cybercrime enforcement, causing ambiguity and inefficiencies. Respondents also highlighted that the current coordination framework leads to delay and regulatory gaps. Establishing a clear coordination framework and investigation protocols such as information sharing, joint investigation between regulators and law enforcement agencies would help in handling complex cases. Issues relating to jurisdictional gaps and duplication of tasks will also be addressed simultaneously, affecting more efficient outcomes for the current issue.

Finally, cross-border identity theft poses a significant challenge to PDPA enforcement due to jurisdiction limitations beyond Malaysian authorities. Many data breaches and online scams originated outside Malaysia were left unaddressed because the domestic authorities had no powers to investigate and prosecute the offenders. Enhancing enforcement also required international cooperation through mutual agreement with other countries and aligned with the standard of international law. Moreover, aligning the data protection principles with the international legal frameworks would improve the effectiveness of data protection regulation across the entire world and minimize more risks as the collaboration of the government authorities.

In conclusion, the Personal Data Protection Act 2010 functions as the primary safeguard for millions of Malaysians. Nevertheless, the said act can be strengthened by drawing lessons from Identity Theft and Assumption Deterrence Act of 1998 in the United States with a victim-centric approach. This is not to suggest that the PDPA is an insufficient and ancient piece of legislation. Rather, it highlights the need for continual reform to fit the ever-growing modern technology, as artificial intelligence continues to dominate the world. Accordingly, this study has achieved its research objectives. By examining both legislative frameworks, this study demonstrates a hybrid legal approach, maintaining regulatory structure of PDPA while including victim-oriented remedies. This can significantly enhance Malaysia's regulations on data protection.

[102] Jillian Chia and Nicole Oh, 'Data Protection & Privacy 2020' (Skrine, 1 January 2020) <https://www.skrine.com/insights/publications/2020/january/data-protection-privacy-2020> accessed 31 December 2025.