Financial Economics Insights

Article

The Ineffectiveness of Current Strategies in Australia Calls for a Comprehensive Anti-Fraud Ecosystem

Siyu Chen [1,*]

[1] University of Sydney, Sydney, Australia
* Correspondence: Siyu Chen, University of Sydney, Sydney, Australia

Abstract: This paper delves into the current status of the online anti-fraud market in Australia, analyzes in detail the ineffectiveness of existing strategies, and the latest actions of the government and businesses in building an anti-fraud ecosystem, so as to objectively show the application process, opportunities and challenges of the anti-fraud regulatory framework in Australia. The author gives shallow suggestions from both the government and businesses' perspectives to facilitate building a comprehensive anti-fraud ecosystem in the future.

Keywords: logit model; financial fraud; discrete choice model; binary classification

Published: 13 November 2024

1. Introduction

Online fraud is now one of the main types of fraud in this age of digital prosperity. While digital adoption and technological advancements have increased convenience, efficiency, and user experience, they have also unintentionally increased opportunities for criminal activity. This increases the frequency and sophistication of online fraud activities. Specifically, fraudsters use the banking sector's quick, seamless online and mobile payment systems to defraud people and organizations by taking advantage of platform vulnerabilities [6]. Unlike traditional fraud, cybercrime is global in nature. International criminal organizations share cutting-edge technology on the dark web, enabling them to launch massive attacks on thousands of Australians simultaneously. The Australian Federal Police (AFP) reports that cyber fraud costs Australia hundreds of millions of dollars annually and has grown to be one of the fastest-growing crime types in the country [5].

Businesses and governments in Australia have responded with initiatives. Nevertheless, these regulatory measures have not stopped online fraud because they have not kept up with the advancement of criminal technology. Current strategies for preventing and compensating victims of online fraud are ineffective. However, this does not imply that all existing strategies are inadvisable; measures in some areas continue to have positive effects. Therefore, I will further assess the current state of online fraud in Australia, identify the factors contributing to its rise, and evaluate the feasibility and limitations of the current commercial and governmental responses. Lastly, considering the shortcomings of the current approach, It's my view that by enhancing laws and regulations, establishing a specialised anti-fraud agency, and stepping up public education on cyber security. the government in Collaboration with businesses, could optimize the protection measures to prevent online fraud.

2. Current Situation of Online Fraud

2.1. Post-Pandemic Rise

With the outbreak of COVID-19, people's social distancing has begun to increase, giving people a reason to spend more time on social media and engage in non-face-to-face online activities [14]. Nowadays, online activities are not limited to chatting and

interacting with friends or strangers online but also include e-commerce sales and even news sources. Social media has gradually integrated into people's daily lives [17]. According to data from Stripe, e-commerce has indeed seen a historic growth after the epidemic. In 2021, the second year after the epidemic, major companies used Stripe to process more than $640 billion in payments, an increase of 60% year-on-year (2022). The huge increase in the number of transactions conducted through online platforms indicates that the number of people using e-commerce is constantly increasing, which provides more opportunities for scammers. Compared with before, the forms of online fraud have become more complex.

2.2. Variety in Forms and Countries

2.2.1. Variety in Forms

Nowadays, online fraud is ubiquitous, increasingly sophisticated and constantly evolving. Today's forms of online fraud include Phishing emails and texts, which trick victims into providing personal information by sending fake emails or text messages. Victims may engage with certain websites or establish connections on social media, trusting these familiar individuals or entities and thereby becoming more likely to disclose their information. For instance, with the continuous development of e-commerce, online banking, investment fraud is on the rise where criminals get victims to invest their money by providing false information about high returns. In online shopping scams, criminals often sell counterfeit or low-quality products. After victims make payments, they may not receive the goods; if they do, the products are typically of substandard quality [14].

Beyond direct monetary scams, criminals may seek to gather sensitive information such as credit card and bank account details. For example, a criminal group called BogusBazaar defrauded tens of millions of dollars through faking shopping websites, affecting up to 850,000 victims. The criminal group used fake websites to sell non-existent or counterfeit products while capturing victims' credit card information. The criminal group is still using other websites to commit fraud and avoid the supervision of law enforcement agencies [12]. It indicates that current strategies might be ineffective against online fraud. The rapid advancement of internet technology has expanded the scope of fraud, and existing strategies cannot track every ‘new-born’ type of transactions. The development of social media has also made it difficult for victims to distinguish the authenticity of the information they have received.

2.2.2. Variety Across Countries

At the same time, Variation of online fraud across nations makes it even difficult for regulators to track and deal with them effectively. Countries like Latin American, are particularly susceptible to online scams, 222% higher than the Asia-Pacific region [18]. The reliance on locally operated payment infrastructures and lower frequency of credit card usage are factors contributing to weaker banking systems. Conversely, businesses in Europe experience significantly lower fraud rates compared to Latin America. This difference is probably because they are subject to the Strong Customer Authentication (SCA) regulations, which mandate businesses to add two-factor authentication in the checkout processes.

3. Current Strategies and Ineffectiveness

The current anti-scam strategies in Australia vary from sector to sector and are mainly focused on separate industries such as telecommunications providers to curtail the prevalence of telecommunications scams in the past few years. The ACMA introduced *the Reducing Scam Calls and Short Messages Code*, which require telecommunications providers to take steps to combat scam calls and messages. Nowadays, however, technology is iterating at an unstoppable pace and reshaping the industry and societal norms. Online scam’s techniques and tactics are increasingly complex together with its transnational and

cross-industry nature, making the existing anti-scam measures less effective than ever, mainly reflecting in the following four aspects:

3.1. Lack of Cross-Industry Collaboration and Unified Standards

Regulatory efforts have already been put in telecommunications sector where telecommunications providers are subject to specific industry codes. Positive outcomes have begun to emerge -- 1.4 billion scam calls and 257 million scam text messages have been successfully intercepted in 2022 [4]. However, with the decreasing number of scam calls, the economic loss caused by scams increased by 40.6%, reaching 141 million dollars [4]. It indicates that scams are now spreading, exploiting vulnerabilities in other affected sectors such as finance and digital platforms where mandatory industry codes have not yet been in place. Scammers cunningly target at inconsistent standards across various industries, carrying out online scams via various platforms. For instance, they first use phishing links to direct victims to a disguised bank or payment platform, and then further obtain identity and financial information for defrauding money. Currently, due to low engagement and inadequate protection from banks and digital platforms, these scams are becoming increasingly difficult to prevent, detect and disrupt in a timely manner, leading to 65 per cent of Australians still exposed to fraud attempts in 2022 [3].

3.2. Consumer Protection and Victim Compensation Mechanism

First, most banks' current strategies are focused heavily on the prevention phase such as the rule-based principles to mark the suspicious clients and transactions, but neglect the overall handling during the aftermath of online fraud, especially victims' compensations. Secondly, although some banks have introduced the *'Scam-Safe Accord'*, such as delaying high-risk payments and confirming the identity of payee [2], the scope is still limited, placing consumers into a disadvantageous position. Additionally, due to the absence of consensus and clear division of responsibilities across bank sectors, banks may pass the responsibility to each other, which leads to lengthy claim procedures such as back-and-forth negotiations across different departments, thus making it rather difficult for affected consumers to obtain timely compensation.

3.3. The Supervision of New Fraud Methods Lags Behind

As mentioned earlier, the government have introduced the *Reducing Scam Short Messages Code* as early as 2021. However, due to the delayed implementation of the code and the slow systematic response, scammers quickly turned to the unregulated third-party messaging platforms. Disguised as governments or well-known companies, they continue to send scam messages containing fake links to defraud users of personal information and bank accounts. Ironically, due to the lag in the regulation against new types of online scams, the loop-hole was not discovered and started to be closed until the end of 2022 [4]. This case clearly illustrates the ineffectiveness of existing strategies to respond to the iterative online scams threats, leaving a large number of users exposed to cyber risks for almost one year.

3.4. Cyber Risks Caused by Backward Technology

The forms of online scams keep evolving, with scammers keep innovating and competing to outpace in scam technologies. The government have found it in a passive and lagging position when it comes to updating regulatory frameworks and responding swiftly to these emerging cyber threats. Regulatory and enforcement efforts often fail to keep pace with the rapid development in scam techniques.

This delay has created serious challenges in combating new forms of online fraud. ACMA pointed out in its *Digital Platform Services Survey* that some scams targeted several emerging digital advertising platforms that are not equipped with mature regulatory norms. In 2022, $80 million in losses to scams were attributed to social media alone, higher

than all other contact methods excluding phone calls [4]. These online platforms are lack of strict identity verification mechanisms and advertising content audit, allowing scammers to post false advertisements for deceiving consumers. However, due to the backward technology, the platforms lack advanced anti-fraud detection tools and data analysis capabilities, thus hampering platforms from identifying and removing deceptive contents. Such technological lags pose serious challenges for governments and businesses to track and block new online fraud effectively.

4. Business and Corporate Measures to Protect Victims

The increase of cyber fraud has caused serious economic losses and psychological trauma to the society and consumers. In order to effectively protect the victims of online fraud and prevent the occurrence of it, the government and businesses need to take a series of comprehensive measures, including some independent measures and government-enterprise cooperation measures.

4.1. Government Measures

4.1.1. Refinement of Legal Framework

From a governmental perspective, the formulation and enhancement of relevant laws and regulations are crucial to safeguarding the interests of the general public and victims of online fraud. For example, the Australian government passed a new bill in June 2024, aiming at cracking down on SMS fraud [15]. Well-refined laws and regulations are the basis of combating online fraud, as the law can clarify the definition, scope, degree of crime and punishment standards of online fraud, and law enforcement agencies provide legal basis. Thus, criminals are likewise subject to legal prosecution and sanction under the law. And victims can be protected by law. Moreover, refining the law helps to raise public legal awareness and strengthen preventative consciousness.

4.1.2. Establishment of Specialized Anti-Scam Agencies

Establishing specialized anti-fraud agencies or enhancing the functions and authority of existing ones can effectively strengthen the supervision and regulation of online fraud. For example, the Australian government established *the National Anti-Scam Centre* to bring together the efforts of the government, law enforcement agencies and private sector experts for combating online scams [16]. The specially-established anti-scam agency is an independent entity. Its independence guaranteed it to focus on anti-scam work with high levels of efficiency and professionalism. Specifically, they can concentrate resources and channels to carry out special attacks on fraud crimes and protect victims. Moreover, anti-scam agencies can also cooperate with other countries and international organizations to share information and technology to jointly combat transnational cyber fraud crimes. Given the transnational nature of cyberfraud crime, international collaboration is essential in effectively addressing this global threat [1]. As Australia faces an increasing number of online fraud cases from abroad, it is far from enough to catch transnational fraudsters by relying solely on domestic laws and regulation efforts. The Australian government should cooperate and share with other countries and international organizations relevant information and technology for joint combat. The advantage of international cooperation is not only to supplement the resource limitations of a single country or organization, but also to improve each country's anti-scam capacity and form a comprehensive global anti-scam ecosystem.

4.1.3. Promotion for Better Public Awareness

Furthermore, the government should work to raise public awareness of online fraud by promoting knowledge about common scam tactics, channels, and potential financial losses, alongside strategies for fraud prevention. Education efforts should particularly focus on minors and the elderly, as these groups are more vulnerable to online scams and thus require targeted awareness initiatives. An easy-to-use online reporting platform is

also preferred as a useful tool as it allows victims to quickly report online scams, enabling governments, businesses and law enforcement to take more timely action, such as the Australian Signals Directorate's online scam Reporting Mechanism and Latest Alerts [8], which allows the public to quickly detect and report online scam. Increasing public awareness of online scams reduces opportunities for scammers to exploit potential victims, thus providing protection against fraud at its source. Great process has been witnessed that *Australian Competition and Consumer Commission(ACCC)* promotes anti-scam knowledge through Scamwatch, social media and email. However, as the ACCC is limited in its ability to assist victims [4], anti-scam education should be carried out in collaboration with government support and specialized anti-scam agencies.

4.2. Businesses Measures

On the other hand, with the vigorous development of the Internet economy, whether for the need of regulatory compliance or to ensure the sound operation of its own business, strengthening online business security protection, preventing and combating online fraud has become an indispensable and important task for enterprises.

4.2.1. Collaboration with Government

First, companies should cooperate with the government. Companies can share information and resources with the government to build a wall of protection against online scams. After a year of heavy losses due to online scams, the Australian government and the banking industry will begin working together to advance anti-scam measures in 2023 [13]. Banks and governments can work together to monitor the flow of money. Notably, it is important for telecommunications providers and communications companies to intercept and track suspicious text messages, calls, emails and Internet links, alert victims of potential online scams, and share this information with government agencies.

4.2.2. Assistance to Victims

Enterprises and the government should cooperate in the support and protection of victims of online scams. In this process, enterprises should provide financial, legal and psychological assistance to victims under the leadership of the government, such as the establishment of foundations and the assistance of lawyers. Collaborative initiatives, such as establishing a victim protection fund with private sector support, can provide compensation and legal aid, ultimately fostering public trust and reinforcing government commitment to victim protection [11].

4.2.3. Internal Measures

Enterprises must implement internal measures to prevent online scams, as combating cyber fraud is the responsibility of every employee. Regular cybersecurity and anti-scam training for staff, reinforced by cybersecurity bulletins and meetings, along with educating customers on cybersecurity's importance [9], can help both employees and clients detect and prevent online scams promptly. Enterprise cybersecurity education contributes to broader societal cybersecurity awareness, making it a shared responsibility of both the organization and its employees. Enhancing cybersecurity training within companies not only strengthens the enterprise's own defenses but also elevates the overall cybersecurity standards of society.

5. Summary

The Australian online anti-fraud market is in a process of dynamic changes and continuous evolution. On the one hand, with the popularization of online transactions, online fraud cases are frequent, showing the urgency of anti-scam market demand; on the other hand, large numbers of technology and service providers are actively responding, and strive to improve the effectiveness of anti-fraud by introducing advanced big data analysis

and artificial intelligence. At the same time, the gradual maturity of the regulatory environment also provides necessary norms for market development. Overall, although the Australian online anti-fraud market faces challenges, it has shown a positive development trend as a whole, and will surely contribute to a more stable and sustainable landscape in the future with the joint efforts of all parties.

Acknowledgments: Thank Professor Xi Nan for offering the kind advice. Also thanks for the hard work of chaichai.

References

1. Arnell P, Faturoti B. The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. Int Rev Law Comput Technol. 2022 Jun 8. Available from: https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2061888
2. Australian Banking Association. New Scam Safe Accord. 2023. Available from: https://www.ausbanking.org.au/new-scam-safe-accord/
3. Australian Bureau of Statistics (ABS). 13.2 million Australians exposed to scams [media release]. 2023 Feb 22. Accessed 2024 Oct 9.
4. Australian Competition and Consumer Commission (ACCC). Targeting Scams. 2023 Apr. Available from: https://www.accc.gov.au/system/files/Targeting%20scams%202022
5. Australian Federal Police. Cybercrime: Combatting a serious criminal threat to Australia and Australians. 2023. Available from: https://www.afp.gov.au/crimes/cybercrime
6. Australia Government Treasury. Scams-Mandatory Industry Codes Consultation paper. 2023. Available from: https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf
7. Australian Government. Types of scams. 2023. Available from: https://www.cyber.gov.au/learn-basics/watch-out-threats/types-scams
8. Australian Signals Directorate. Australian Government. 2024. Available from: https://www.cyber.gov.au/
9. Business Queensland. Keeping Your Business Cyber Secure. Queensland Government. 2024 Aug 13. Available from: https://www.business.qld.gov.au/running-business/digital-business/online-risk-security/cyber-security
10. Berrill & Watson. Can I get compensation for losses due to a scam? 2023 Feb 20. Available from: https://www.berrillwatson.com.au/supertalk-blog/2023/february/scam-compensation/
11. Cross C, Richards K, Smith R. The reporting experiences and support needs of victims of online fraud. Australian Institute of Criminology. 2016 Aug 11. Available from: https://www.aic.gov.au/publications/tandi/tandi518
12. Connatser M. What do Europeans, Americans and Australians have in common? Scammed $50M by fake e-stores. The Register. 2024 May 8. Available from: https://www.theregister.com/2024/05/08/bogusbazaar_fraud_china/
13. Hilder K, Doherty S. Combatting Online Scams: Government and the Banking Sector Announce New Measures. MinterEllison. 2023 May 18. Available from: https://www.minterellison.com/articles/combatting-scams-new-government-and-industry-measures-announced
14. IFEC. Beware of online scams - IFEC. 2021 Mar 9. Available from: https://www.ifec.org.hk/web/en/moneyessentials/scams/scam-websites.page
15. MP Rowland M. New legislation to crack down on SMS scams. Ministers for Infrastructure, Transport, Regional Development, Communications and the Arts. 2024 Jun 26. Available from: https://minister.infrastructure.gov.au/rowland/media-release/new-legislation-crack-down-sms-scams
16. National Anti-Scam Centre. Australian Government. 2024. Available from: https://www.nasc.gov.au/
17. Statista. Topic: Social media in Australia. 2022 Apr 1. Available from: https://www.statista.com/topics/8628/social-media-in-australia/#topicOverview
18. Stripe. Stripe: The state of online fraud. 2022. Available from: https://stripe.com/au/guides/state-of-online-fraud
19. Sukianto A. 10 Ways to Reduce Cybersecurity Risk for Your Organization. UpGuard. 2024 Sep 16. Available from: https://www.upguard.com/blog/reduce-cybersecurity-risk