Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD29257

Research on Money Laundering in Live Streaming Platforms: Analysis of Criminal Mechanisms, Detection Methods, and Regulatory Challenges

Zichen Ling

Seventh College, University of California, San Diego, USA
z2ling@ucsd.edu

Abstract. Live streaming platforms have become an important part of the digital entertainment economy, forming close connections with users through interactive functions and diversified monetization tools. However, the unique multi-account transaction chains, virtual gifts, and distributed reward mechanisms of live streaming platforms significantly increase the complexity of financial risk management, creating new compliance and regulatory challenges. This paper systematically reviews the potential types of financial risks associated with live streaming platforms, evaluates the applicability of existing detection methods, and compares regulatory models across different jurisdictions. The study finds that the real-time and micro-transaction characteristics of live streaming make the application of traditional anti-money laundering (AML) frameworks subject to delays and insufficient coverage. Taking China and Western countries as examples, China has implemented stricter measures in real-name authentication and platform responsibility systems, while Western jurisdictions mainly rely on financial institutions' risk assessments and reporting mechanisms. This paper proposes an integrated risk management framework that combines behavioral analysis, network analysis, and cross-platform regulatory collaboration to enhance the monitoring of complex transaction structures. At the same time, it recommends that regulators adopt adaptive regulatory strategies to cope with the rapidly evolving compliance challenges in live streaming environments.

Keywords: live streaming platforms, financial compliance, digital payments, anti-money laundering, regulatory framework

1. Introduction

As the digital economy grows rapidly, live streaming services have become a part of the online entertainment and socialization. expanded their user base and continued to inspire the development of new transaction models including virtual gifts, point redemption, and cross-border payments through the instant interactivity and various monetization mechanisms. But as these innovations spur economic growth they also create more complex financial risks. The flow of funds is often hard to track due to information asymmetry, multi-account systems, and the lack of transparency of virtual currencies, which only exacerbates compliance and regulatory issues. It has also been pointed out by international organizations that cross-border virtual payments and micro-transactions have taken a significant role in financial crime and money laundering and are a direct challenge to current compliance systems.

It is in this context that the conventional systems of anti-money laundering and risk control are becoming more and more limiting. Even though statistical approaches, machine learning, and network analysis have enhanced the detection features to a reasonable degree, they are still too weak to meet the requirements of real-time and high-frequency transactions of live streaming. Besides, the variations in the regulatory models among nations also make cross-border compliance more difficult. China has seen some success in preventive efforts with real-name registration and platform responsibility systems, in contrast to Western jurisdictions, where the risk reporting and ex-post compliance of financial institutions are the focus. At the same time, the global governance faces new challenges due to judicial conflicts associated with cross-border movement of funds, a lack of data sharing, and the protection of privacy.

The management of financial risk in live streaming platforms is not just an immediate necessity of the development of the industry, but also an important task of protecting financial stability and social confidence. The example of common judicial proceedings demonstrates that the livestreaming rewards can be used as a medium of money laundering, and the investigation in the industry suggests that virtual transactions are still occupied with an expanding portion of economic crimes. U.S. Department of Justice enforcement documents also show that there are loopholes in how cross-border payments using virtual currencies are enforced. Thus, the investigation of financial risk management and compliance issues in live streaming platforms not only expands the theoretical discussion of the specified issue of digital finance but also offers practical policy guidelines to regulators and the operators of the platforms.

2. Literature review

2.1. Financial risk characteristics of live streaming platforms

Traditional financial risk theories usually focus on information gaps, moral hazard, and systemic risk in banks and other old-style financial institutions. However, with the rise of digital platforms, these ideas do not always fit. The platform economy brings new features such as network effects, algorithmic intermediation, and virtual asset circulation that challenge classical risk assessment frameworks. Some scholars point out that the “just-in-time” nature of platform transactions creates unprecedented volatility in fund flows. Others note that the hidden nature of algorithms makes the gap in information between users and platform owners even wider [1]. These insights suggest that models built for traditional finance may not fully capture the fast-changing and spread-out world of platform transactions.

The live streaming economy has further complicated this landscape through the introduction of virtual gift economies and multi-tiered monetization structures. Relevant research has established that two-sided network effects create complex interdependencies between content creators and consumers, generating transaction patterns that defy conventional monitoring approaches [2]. In live streaming contexts, virtual gifts serve not merely as digital commodities but as potential vehicles for value transfer that exist in regulatory gray zones. The conversion mechanisms between virtual currencies, platform points, and fiat money create multiple layers of abstraction that obscure the ultimate source and destination of funds. Recent studies indicate that these virtual economies can facilitate complex intermediary structures involving up to seven distinct layers, with each additional tier introducing greater transactional opacity and progressively undermining the effectiveness of conventional anti-money laundering detection systems.

The evolutionary trajectory from traditional e-commerce to live streaming platforms represents a qualitative shift in financial risk exposure. Early digital platforms operated primarily as marketplaces with relatively transparent transaction structures. However, current live streaming platforms integrate social interaction, entertainment, and commerce into the experience. Financial transactions gradually occur as byproducts of social engagement rather than deliberate commercial activities. This integration creates "embedded finance," where monetary exchanges become deeply woven into social interactions that users may not perceive as financial activities requiring regulatory oversight. The OECD Digital Economy Outlook 2021 emphasizes that this embeddedness poses fundamental challenges to regulatory visibility, as traditional transaction monitoring systems are designed to flag explicit financial operations rather than socially-motivated micro-transactions that may collectively represent significant fund movements.

2.2. Detection methods and regulatory frameworks

2.2.1. Detection methods

Three major technological options are used to detect financial crimes in the virtual world, each having its own capabilities and drawbacks. Anomaly detection is based on statistical methods, which use outlier analysis, clustering, time-series modeling, and other techniques to detect transactions that do not follow the existing patterns. Such methods are good at identifying gross anomalies, including transactions that are unusually large or bursts of activity, but are not as good at more complex schemes that act very much like legitimate behavior [3]. According to OECD research, statistical techniques often involve heavy historical data to determine baseline patterns, which makes them ineffective in new platforms or in fast-growing types of transactions. Also, these techniques tend to produce large false-positive rates in the context of live streaming, where the behavior of the users naturally has a high degree of variability because of viral content, appearances of celebrities, or promotions.

The second generation of detection tools is machine learning and big data analytics, which offer superior pattern recognition features via neural networks, random forests, and ensemble approaches [4]. According to FATF reports, these methods are capable of handling large amounts of transactions almost in real-time, tracking complicated patterns that human analysts or other statistical tools would otherwise not discover. More sophisticated applications use natural language processing to process chat messages, computer vision to process streaming content, and graph neural networks to learn transaction relationships. These advanced tools, however, are difficult to effectively use in live streaming settings because of data quality, large labeled training data requirements, and because many machine learning models are black box, making it difficult to meet regulatory requirements. KPMG studies have shown that machine learning systems need to be continually retrained to suit changing criminal trends, which introduces a cost of ongoing operation and computation, which small platforms might be unable to sustain.

The third pillar of detection frameworks is network analysis methods that aim to expose account relationships, find coordinated behavior, and trace fund flow paths. These methods model the transactions as a graph with nodes representing an account and edges a financial relation, allowing the identification of suspicious patterns (e.g., circular transactions, layered transfers, or focal point collection). PwC research shows that network analysis is capable of identifying money laundering operations that cut across accounts and platforms to show structures not observed in transaction-based analysis. The success of network approaches is, however, highly reliant on inter-platform and inter-jurisdictional integration of data- a demand that is incompatible with data protection and competitive provisions. In addition, advanced actors are increasingly applying methods to break up their networks, by using a large number of low-value intermediary accounts to hide eventual beneficial ownership and circumvent graph-based detection.

2.2.2. Regulatory frameworks

While detection methods provide the technical foundation for identifying suspicious activities, their effectiveness depends heavily on the regulatory frameworks within which they operate. Regulatory frameworks exhibit significant variation across jurisdictions, reflecting different philosophical approaches to platform governance and financial oversight. China already has a fully adopted system that focuses on real-name registration and platform responsibility systems, as well as active monitoring. In 2021, the Supreme People's Court of China fixed that platforms have a collective responsibility to enable financial crimes where they do not install sufficient controls and this creates a strong incentive to take risks aggressively. This strategy is focused on prevention and early detection, which means that platforms must authenticate the user and track their activity patterns and report any suspicious behavior in real-time. The International Monetary Fund notes that the model of China has high compliance rates yet raises issues regarding privacy, data safety and that regulatory overreach can occur, which has the possibility of stifling innovation.

Conversely, Western regulation generally assigns westernized platforms and traditional financial institutions roles and responsibilities, with the focus being on ex-post detection and reporting, instead of ex-ante prevention. The 2022 Anti-Money Laundering Package of the European Commission preserves this principle by imposing primary implications of AML on banks and payment processors and considering platforms as businesses and not as dealing with quasi-financial institutions [5]. The solution retained innovation on the platform and avoided user privacy, but could leave loopholes in regulations, especially in closed-loop virtual economies where money does not flow through banks. Research by the World Bank suggests that Western paradigms presuppose strong information disclosure between platforms and financial institutions, which is progressively doubted by encryption, privacy laws, and the internationalisation of digital services. Altogether, those regulatory distinctions directly affect the efficiency of financial risk prevention and detection instruments and, at the same time, can open opportunities to cybercriminal individuals to commit fraud and abuse regulatory requirements. The fragmentation between national regulatory regimes creates arbitrage opportunities where sophisticated actors exploit jurisdictional differences to evade detection.

3. Results and discussion

3.1. Analysis of financial risk mechanisms in live streaming platforms

Live streaming sites have a complicated risk structure with three main structural weaknesses, i.e. many-account systems that allow (the task of) identity fragmentation, virtual gift economies that promote value transfer coding, and cross-platform funds transfers that take advantage of regulatory arbitrage possibilities. The architecture operative in the live streaming platforms is associated with the formation of several layers of obscurantism, which are the major hosts of racism types that define live streaming systems and their inherent conflict with traditional financial surveillance processes. Multi-account systems, when under a single user, permit multiple personas where individuals can use the system with a separate set of wallets, transaction histories, and activity behavioral patterns that hide the aggregation of interests behind the debited controller. Studies have shown that this fragmentation is a reflection of corporate veil techniques used in traditional money laundering, and exists on an unprecedented scale and speed, attributed to the low barriers to account creation associated with digital settings [6]. Virtual wallets are becoming particularly problematic because they introduce intermediary disparities centered on the block, which exist within platform-echo systems and may never translate to fiat and therefore escape the scrutiny of conventional banking procedures. The overlaps between these systems allow complex layering structures of this nature, in which illicit funds can be cascaded masked in dozens of accounts, exchanged masked in a variety of types of virtual assets, and ultimately aggregated with apparently legitimate withdrawal patterns that in turn each fall below a reporting level.

The very nature of virtual gift economies as both a social signaling system and a value transfer system draws especially high risks because of their dual character. The applicable literature shows that virtual gifts on live streaming communities may be used as instruments in de facto bearation-transferable forms of stores of value likened to those in bearer warehous- that need nearly no traceability. This feature is taken advantage of by criminal actors, who buy the virtual gifts with the help of illicit money and transfer them to accomplice accounts in the guise of a genuine streamer and then redeem them using the platform's revenue-sharing features that look to be the kind of legitimate entertainment revenue [7]. Card Social Gift-giving offers a natural protection of these transactions, with massive gifts to prominent streamers being in line with the fan behavior instead of financial mischief. In addition, the secondary markets which has developed around virtual gifts: where users can exchange gifts between each other at a visible discount, add a further layer of complexity that allows an equivalent of cryptocurrency tumblers by mixing values.

The third major structural vulnerability is cross-platform and cross-border fund transfers, which give jurisdictional arbitrage opportunities that capitalize on regulatory fragmentation. Looking around the live platforms, the UNODC 2020 Global Report on Financial Crime explains that live streaming sites are highly vulnerable to transnational money laundering because it can be used to transfer the value instantly across borders without any traditional relations with a correspondent bank [8]. There is an upsurge in the recently used strategies of criminal networks in which the money enters the system in jurisdictions with little to no platform regulation, moves across a number of platforms and virtual asset converters, and comes out of them in jurisdictions with a high level of privacy protection or limited participation in enforcement. These schemes are made possible by the technical architecture of contemporary platforms through the use of APIs and payment gateways to seamlessly interconnect services over the borders of regulations. Additionally, some platforms store information in cryptocurrency and as an intermediate, which further increases the degree of obfuscation, since blockchain transactions, though theoretically transparent, in practice offer significant levels of anonymity due to mixers and privacy coins.

3.2. Detection challenges and regulatory responses

The inherent incongruence between the old systems of anti-money laundering and live streaming transactions poses systematic loopholes in the detection of financial crime. Traditional AML structures frequently use the periodic reporting of suspicious activity, usually on a daily or weekly basis, where financial institutions compile suspicious activity reports on the basis of threshold analysis and pattern identification. Nevertheless, live streaming transactions are settled instantly and in real time, which means that criminal actors can accomplish the layering and integration processes in minutes or hours, long before traditional detection procedures would identify the activity [9]. The

European Commission acknowledges in its research that this temporal misalignment represents a critical vulnerability, as delayed detection often means that funds have already been converted, transferred, or withdrawn by the time authorities receive alerts.

Most live-streaming payments are very small, often less than one dollar. This makes it easier for criminals to avoid traditional monitoring systems, which usually focus on large transactions. By splitting big sums into many small ones, they escape detection. A review of regulatory strategies shows a trade-off between effectiveness and practicality. In China, regulators focus on ex-ante measures. These include mandatory real-name registration and legal responsibility for platforms. Such rules create strong deterrent effects. They also allow authorities to act quickly when unusual activity appears. Case records from the Supreme People’s Court show that monitoring systems have frozen suspicious accounts within hours of detection, stopping money laundering before it was completed [10]. At the same time, this model depends on complex technical systems. It creates high compliance costs for platforms. It also raises concerns about government surveillance and user privacy. The system’s success relies on strong identity checks. Yet fake documents or stolen identities can still bypass these measures, especially in places where protections against identity theft are weak. To address these problems, scholars and policymakers suggest stronger tools. Proposed measures include biometric authentication and greater cooperation across platforms.

Western regulatory models prioritizing institutional compliance and ex-post supervision offer greater flexibility and lower barriers to platform innovation but may sacrifice detection timeliness and coverage. The U.S. Department of Justice Virtual Currency Enforcement Framework acknowledges that reliance on financial institutions' risk assessments creates blind spots when platforms operate closed-loop economies or utilize unregulated payment channels [11]. This approach assumes that funds will eventually interface with regulated financial institutions, triggering AML controls at that point. However, the emergence of cryptocurrency withdrawal options and peer-to-peer cash-out networks increasingly allows criminals to bypass traditional banking entirely. PwC's Global Economic Crime Survey indicates that Western jurisdictions are experiencing rising detection latency—the time between criminal activity and regulatory awareness—as platforms evolve faster than regulatory adaptation.

Cross-border enforcement is likely to be the least straightforward since financial crime has safe havens due to the jurisdictional issues, data protection, and absence of information-sharing mechanisms. International crime participation structures, such as mutual legal assistance treaties (MLATs) have been created on the premise of outdated criminal investigation processes that require months at a time to conclude, instead of the real-time enforcement demands of digital financial crime. The necessity to work with different laws in different jurisdictions, to apply to the court with diverse orders in different jurisdictions and alliance on conflicting privacy rules means that global enforcement action may require several years to be accomplished. Meanwhile, criminals exploit these delays to move across borders as fast as possible. They often use platforms in non-cooperative jurisdictions [12]. They may also design operations so that evidence and assets are spread across different countries. Even when cooperation exists in principle, practical barriers remain. Language differences, conflicting evidentiary standards, and varying definitions of financial crimes all make collaboration more difficult.

3.3. Case studies and empirical evidence

The "live streaming reward money laundering case" prosecuted in China provides detailed insights into the operational sophistication of platform-based financial crime. In this scheme, criminal organizations established networks of fake streamer accounts that broadcast low-quality or automated content while confederates posing as viewers sent large volumes of virtual gifts purchased with funds from fraud, corruption, and drug trafficking. Supreme People's Court case files reveal that this large-scale operation involved hundreds of accounts across multiple platforms, processing tens of millions of dollars over 18 months. The criminals employed sophisticated techniques to evade detection, including staggered transaction timing to avoid velocity checks, geographic distribution of accounts to prevent pattern recognition, and deliberate mixing of illicit funds with legitimate viewer gifts to obscure the criminal proceeds. The multi-layer cashing-out process involved initial conversion of gifts to platform points, transfer to virtual wallets, gradual withdrawal in amounts below reporting thresholds, and final collection through a network of money mules recruited via social media.

The case demonstrated critical vulnerabilities in platform compliance systems, particularly the inadequacy of identity verification processes that allowed single individuals to control multiple accounts using purchased or stolen credentials. Forensic analysis revealed that transaction monitoring algorithms failed to correlate activities across related accounts because platforms treated each account as independent, missing the consolidated pattern that would have clearly indicated money laundering. Furthermore, the revenue-sharing model that treated streamer earnings as legitimate business income enabled the criminals to obtain official payment records and tax documentation that gave their illicit proceeds the appearance of legal entertainment revenue. The investigation required extensive cross-platform cooperation and data correlation that platform operators initially resisted due to competitive concerns and privacy considerations, delaying detection by an estimated 11 months during which the criminal network expanded operations. While Chinese and Western cases reveal similar underlying vulnerabilities in platform-based financial crime, they demonstrate distinct operational methods and regulatory gaps that criminals exploit.

Cross-border virtual currency cases in Western jurisdictions illustrate different but equally concerning vulnerabilities in international financial crime enforcement. Cases from the U.S. Department of Justice illustrate how criminals have exploited live streaming platforms as a way for money laundering to make their money gained from ransomware attacks legal. The methods relied on several steps. Criminals first bought cryptocurrency. They then converted these assets into virtual gifts on platforms based in Southeast Asia. Finally, they withdrew the value through peer-to-peer cryptocurrency exchanges that operated outside traditional banking oversight. This scheme took advantage of regulatory gaps. U.S. authorities had no direct access to transaction data from foreign platforms [13]. Regulators in Southeast Asia did not classify virtual gifts as financial instruments subject to AML rules [14]. Many cryptocurrency exchanges also worked in legal gray zones without clear licensing standards [15]. The multi-stage cycle created layers of obscurity. Funds moved from fiat currency to cryptocurrency, to virtual gifts, back to cryptocurrency, and finally to fiat currency. These steps made it harder for both blockchain analysis and traditional financial monitoring to follow the money.

The empirical evidence from these cases reveals some common patterns in criminal exploitation of platform vulnerabilities. Both cases involved sophisticated understanding of regulatory boundaries and technical capabilities to structure operations that remained just below detection thresholds or exploited coordination failures between oversight bodies [16]. Criminals demonstrated adaptive behavior, rapidly shifting tactics when platforms enhanced controls in one area, such as moving from large gift transactions to high-volume micro-gifts when velocity limits were implemented. The cases also highlight the critical importance of human intelligence and informant cooperation in detection, as technical systems alone proved insufficient to identify these schemes [17]. In the case of China, detection occurred only after a money mule chose to cooperate with authorities. In the United States, the case advanced when a ransomware victim traced the payments to the live streaming platform. These examples show that technical tools for compliance are important, but not enough. Effective oversight also requires human involvement, intelligence-driven investigations, and stronger systems for cross-border cooperation.

4. Conclusion

This research establishes that live streaming platforms present fundamentally new challenges to financial crime prevention that cannot be addressed through incremental improvements to existing frameworks. The complex transaction structures—characterized by multi-account systems, virtual gift economies, and cross-border fund flows—create opacity that systematically defeats traditional anti-money laundering mechanisms. Comparative analysis reveals that China's preventive approach through real-name verification achieves higher detection rates, while Western models emphasizing institutional compliance better preserve innovation but sacrifice timeliness. Neither approach adequately addresses cross-border dimensions where jurisdictional fragmentation creates enforcement gaps.

The integrated risk management framework proposed combines three essential elements: enhanced behavioral pattern recognition incorporating contextual factors beyond simple threshold analysis; comprehensive network relationship modeling, mapping social connections across accounts; and cross-platform regulatory cooperation mechanisms with standardized data formats. Future research should prioritize technical integration of artificial intelligence beyond supervised machine learning, expanded cross-national comparative studies, and interdisciplinary approaches combining criminology, computer science, and legal scholarship to develop comprehensive theoretical frameworks for understanding platform-based financial crime.

This study faces limitations, including restricted data availability, potential non-representativeness of case studies, and temporal constraints as technologies evolve rapidly, necessitating continued research to address these evolving challenges.

References

[1] De Stefano, V. (2016). The rise of the "just-in-time workforce". International Labour Review, 155(4), 471–502.

[2] Parker, G. G., & Van Alstyne, M. W. (2005). Two-sided network effects: A theory of information product design. Management Science, 51(10), 1494–1504.

[3] Chen, B., Yang, X., & Ma, Z. (2022). Fintech and Financial Risks of Systemically Important Commercial Banks in China: An Inverted U-Shaped Relationship. Sustainability, 14(10), 5912.

[4] Cheng, M., & Qu, Y. (2020). Does Bank FinTech Reduce Credit Risk? Evidence from China. Pacific-Basin Finance Journal, 63, 101398.

[5] Pavlidis, G. (2023). Deploying Artificial Intelligence for Anti-Money Laundering and Asset Recovery: The Dawn of a New Era. Journal of Money Laundering Control, 26(7), 155-166.

[6] Murinde, V., Rizopoulos, E., & Zachariadis, M. (2022). The Impact of the FinTech Revolution on the Future of Banking: Opportunities and Risks. International Review of Financial Analysis, 81, 102103.

[7] Supreme People's Court of China. (2021). Typical Cases on Financial Crimes in Digital Platforms.

[8] Chen, X., You, X., & Chang, V. (2021). FinTech and Commercial Banks' Performance in China: A Leap Forward or Survival of the Fittest? Technological Forecasting & Social Change, 166, 120645.

[9] Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy. BIS Papers, No. 117.

[10] Pistor, K. (2020). The Code of Capital: How the Law Creates Wealth and Inequality. Princeton University Press.

[11] Zetzsche, D., Buckley, R., Arner, D., & Barberis, J. (2020). Regulating digital finance. University of Hong Kong Law Working Paper.

[12] Deng, L., Ye, Q., Xu, L., & Zhou, W. (2021). Fintech and Systemic Risk: Evidence from China. Journal of Financial Economics, 142(1), 145-172.

[13] Pol, R. F. (2020). Anti-Money Laundering: The World's Least Effective Policy Experiment? Together, We Can Fix It. Policy Design and Practice, 3(1), 73-94.

[14] Ferwerda, J., & Reuter, P. (2024). National Assessments of Money Laundering Risks: Stumbling at the Start. Risk Analysis, 44(7), 1589-1605.

[15] He, Z., Huang, J., & Zhou, J. (2023). Open Banking: Credit Market Competition When Borrowers Own the Data. Journal of Financial Economics, 147(2), 449-474.

[16] Najaf, K., Subramaniam, R. K., & Atayah, O. F. (2022). Understanding the Implications of FinTech Peer-to-Peer (P2P) Lending During the COVID-19 Pandemic. Journal of Sustainable Finance & Investment, 12(1), 87-102.

[17] Levi, M. (2020). Evaluating the Control of Money Laundering and Its Underlying Offences: The Search for Meaningful Data. Asian Journal of Criminology, 15, 301-320.