Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 10, No. 1, February, 2026

Digital Financial Compliance Challenges: Applying Routine Activity Theory to Online Gambling Networks Analysis

Rizal Mawardi [1*], Vira Nuraeni [2], Jasman Jasman [1], Huda Trihatmoko [1], Fangky A. Sorongan [1*], Septian Aripin [1], Syaefulloh Maulana Malik [1]

[1] *Faculty of Economics and Business, Perbanas Institute, Jakarta, Indonesia.*

[2] *Indonesian Financial Transaction Reports and Analysis Centre (INTRAC), Jakarta, Indonesia.*

Abstract

This study examines Indonesia's Financial Intelligence Unit (INTRAC) "follow the money" investigative techniques through Routine Activity Theory, analyzing criminal convergence in online gambling money laundering operations. Using qualitative methodology with interviews, observation, and document analysis (December 13-19, 2024), the research applied Cohen and Felson's framework to understand criminal patterns in digital financial ecosystems. Data analysis using Audit Command Language (ACL) revealed criminal convergence patterns where motivated offenders (84.63% male, 50% private sector employees, 53% aged 20-30) exploited digital infrastructure vulnerabilities. Sophisticated schemes included multiple nominee accounts, 5-8 layered transactions, and cryptocurrency laundering in low-surveillance environments. Transaction analysis showed expanding criminal opportunities, increasing to IDR 691.88 trillion (2017-2024). The study demonstrates how digital transformation creates suitable targets faster than regulatory adaptation. Research contributes theoretical insights explaining financial irregularity patterns through routine activity theory while offering practical risk reduction models for global financial intelligence units, advancing regulatory compliance theory and digital financial risk prevention.

Keywords:

Routine Activity Theory;
Digital Financial Compliance;
Money Laundering Detection;
Online Gambling Networks;
Financial Intelligence Unit.

Article History:

Received:	11	September	2025
Revised:	11	December	2025
Accepted:	24	December	2025
Published:	01	February	2026

1- Introduction

The proliferation of digital financial technologies has fundamentally transformed the landscape of financial crime, creating unprecedented challenges for regulatory compliance and law enforcement worldwide [1, 2]. Online gambling represents a particularly complex manifestation of this phenomenon, serving simultaneously as both a predicate offense and a sophisticated money laundering vehicle that exploits the anonymity and speed of digital payment systems [3, 4]. This convergence of technological advancement and criminal innovation necessitates a comprehensive theoretical framework to understand and combat emerging patterns of financial misconduct in cyberspace.

Indonesia presents a critical case study for examining these challenges, as the nation experiences exponential growth in online gambling activities despite stringent legal prohibitions and extensive regulatory interventions. Based on Figure 1, the Ministry of Communication and Informatics blocked over 2.86 million online gambling websites between July 2023 and August 2024, yet Indonesian Financial Transaction Reports and Analysis Center (INTRAC) data reveals a persistent increase in transaction volumes, reaching 168 million transactions worth IDR 327 trillion in 2023 alone. This paradox—where enforcement efforts intensify while criminal activities expand—underscores fundamental gaps in our understanding of digital financial crime dynamics and the effectiveness of traditional regulatory approaches.

* **CONTACT**: rizal.mawardi@perbanas.id; f.sorongan@perbanas.id

DOI: http://dx.doi.org/10.28991/ESJ-2026-010-01-015

Figure 1. Statistics on the Value and Number of Online Gambling Transactions

Existing scholarship on financial crime has established important foundations for understanding money laundering mechanisms [5, 6]. However, these frameworks were developed primarily for conventional banking systems and struggle to address the unique characteristics of digital financial ecosystems [6, 7]. Recent studies have examined specific aspects like cryptocurrency's role [1] and online gambling's transformation [3], yet these contributions remain fragmented.

Current research lacks integrated theoretical frameworks explaining how motivated offenders, suitable targets, and absent guardianship converge specifically in digital financial contexts. While Routine Activity Theory has been applied to cybercrime generally [8], its application to sophisticated financial crime networks involving online gambling and multi-layered money laundering remains underdeveloped. Williams [9] noted that conventional criminological theories inadequately address the spatial and temporal characteristics of digital crime environments. Existing studies predominantly rely on secondary data analysis or simulation models, lacking direct access to financial intelligence unit investigative processes and real-world transaction data. Savona & Riccardi [10] emphasized this methodological gap, arguing that effective anti-money laundering research requires collaboration between academics and practitioners. The overwhelming majority of research focuses on Western financial systems, with limited attention to emerging markets where digital financial crime may manifest differently [11, 12].

This study addresses these gaps by investigating how Routine Activity Theory explains criminal convergence patterns in Indonesia's online gambling money laundering networks, specifically examining INTRAC's "follow the money" investigative techniques. The research pursues three primary objectives. First, to develop an integrated analytical framework demonstrating how motivated offenders systematically exploit suitable targets in low-guardian digital environments. Second, to provide detailed evidence of criminal modus operandi, transaction patterns, and network structures through direct analysis of financial intelligence unit investigative processes and comprehensive transaction data spanning 2017-2024. Third, to generate actionable intelligence for financial regulators and law enforcement agencies globally.

Indonesia's unique position as the world's fourth most populous nation with rapidly expanding digital infrastructure creates ideal conditions for examining digital financial crime convergence. The country experienced 205% growth in online gambling transactions during 2020 alone, accelerating to 674% growth in 2021—increases coinciding with COVID-19 pandemic restrictions [13]. INTRAC operates at the intersection of these challenges, serving as Indonesia's financial intelligence unit responsible for analyzing suspicious transaction reports. The organization processed 52,244 gambling-related suspicious transaction reports in 2024—representing 41.6% of all suspicious activity reports.

Despite theoretical advances, significant gaps remain in understanding how Routine Activity Theory explains financial crime patterns in digital gambling contexts. Our research addresses these gaps by developing an integrated analytical framework demonstrating how all three components interact specifically in online gambling money laundering networks.

Our theoretical contribution extends existing scholarship in three ways. First, we demonstrate that digital transformation creates suitable targets exponentially faster than regulatory adaptation can develop capable guardianship—a temporal asymmetry explaining why financial crime proliferates despite enforcement efforts. Second, we reveal how motivated offenders organize into sophisticated networks that systematically probe guardianship weaknesses. Third, we show that effective countermeasures require restructuring opportunity environments to make entire categories of offenses substantially more difficult.

2- Literature Review

2-1- Routine Activity Theory: Foundations and Evolution

Routine Activity Theory, originally formulated by Cohen & Felson [14], revolutionized criminological thinking by shifting focus from criminal motivation to opportunity structures. The theory posits that crime occurs when three elements converge in time and space: a motivated offender willing to commit a violation, a suitable target available for victimization, and the absence of capable guardianship to prevent the offense. This framework has profound implications for understanding crime patterns and developing prevention strategies, particularly for financial crime where motivations remain constant but opportunities vary dramatically based on technological infrastructure [15].

Cohen & Felson's original formulation focused on predatory street crime, but subsequent scholarship has extended the theory to diverse contexts [14]. Eck & Weisburd [16] applied it to problem-oriented policing, while Grabosky [17] examined white-collar crime, revealing how corporate environments create suitable targets while weak regulatory oversight constitutes absent guardianship. Most relevant to our research, several scholars have adapted Routine Activity Theory to cybercrime and digital environments.

2-2- Routine Activity Theory in Digital Contexts

The application of Routine Activity Theory to cyberspace requires reconceptualizing its core components to account for digital environments' unique characteristics. Yar [18] pioneered this adaptation, arguing that physical space constraints no longer limit criminal opportunities—offenders can simultaneously target millions of victims globally while remaining geographically distant.

Leukfeldt [8] advanced this work by examining cybercrime through all three Routine Activity Theory components. His research demonstrated that motivated offenders in cyberspace include both traditional criminals and technically skilled individuals who exploit system vulnerabilities. Suitable targets encompass organizational systems, digital assets, and information databases. Capable guardianship extends to technical safeguards, institutional mechanisms, and individual protective behaviors.

Buil-Gil et al. [19] contributed important refinements investigating fear of economic cybercrime across Europe. Their findings revealed that guardianship operates differently online—traditional protective factors lose relevance while technical literacy and institutional trust become paramount. Yar [20] extended Routine Activity Theory to online identity theft, demonstrating how digital environments create expanding pools of suitable targets.

2-3- Financial Crime and Money Laundering: Theoretical Perspectives

Money laundering theory has evolved considerably since its initial conceptualization in the 1980s. Traditional frameworks emphasized the three-stage process—placement, layering, and integration—as described by Europol [5] and Fanusie & Robinson [6] guidelines. However, this linear model inadequately captures contemporary money laundering's complexity.

Recent scholarship has developed more sophisticated approaches. Levi & Reuter [21] proposed a market-based framework analyzing money laundering as a specialized service industry. Savona & Riccardi [10] advanced a network analysis approach, demonstrating that money laundering effectiveness depends on structural positions within criminal-legitimate business networks. This network perspective aligns well with Routine Activity Theory—professional facilitators serve as suitable targets that motivated offenders exploit, while regulatory oversight constitutes capable guardianship.

2-4- Online Gambling and Financial Crime Convergence

Online gambling represents a complex intersection of digital technology and financial crime. Gainsbury et al. [3] documented how internet-based platforms transformed gambling from location-restricted activities to ubiquitous services accessible via smartphones. McMullan & Rege [4] demonstrated that gambling platforms serve triple functions: as profit-generating businesses, money laundering vehicles, and recruitment mechanisms for broader criminal networks.

Fiedler [22] contributed theoretical work comparing gambling and financial markets from regulatory perspectives, revealing structural similarities but fundamentally different regulatory approaches. This regulatory gap creates criminal opportunities that sophisticated operators exploit. Europol [5] identified common laundering methods including chip dumping, bonus abuse, and collusive play, though these studies typically rely on regulatory documents, missing sophisticated operations that evade detection.

2-5- The "Follow the Money" Investigative Approach

The "follow the money" investigative philosophy has become central to modern financial crime enforcement. The approach prioritizes tracing illicit assets over identifying perpetrators, based on recognition that financial motivations drive most organized crime [23].

Sutrisni & Sukranatha [24] provided early Indonesian scholarship on this approach, arguing that asset tracing offers strategic advantages including reduced confrontation risks and potential for substantial recovery. Levi & Soudijn [23] conducted comparative analysis across European jurisdictions, finding that countries with strong asset recovery frameworks achieved better organized crime disruption. van Duyne et al. [12] examined practical challenges including technical difficulties in tracing cryptocurrency transactions and legal obstacles in obtaining cross-border financial information.

3- Research Methodology

3-1- Research Design and Philosophical Approach

This study employs qualitative methodology grounded in post-positivist epistemology, acknowledging that social phenomena can be understood through interpretation of subjective experiences and contextual meanings [25]. Our approach aligns with interpretive traditions emphasizing deep engagement with research participants. We selected case study design for several reasons articulated by Yin (2018) [26]. First, our research questions focus on "how" and "why" questions. Second, we examine contemporary phenomena where boundaries between phenomenon and context are not clearly evident. Details of INTRAC respondents and interview sessions are shown in Table 1.

Table 1. List of Research Informants

No.	Informant Name (Initials)	Title/Position	Informant Code	Interview Time
1	GS	Associate Financial Transaction Analyst	A1	13 Dec 2024
2	DS	Junior Financial Transaction Analyst	A2	19 Dec 2024
3	TN	Junior Financial Transaction Analyst	A3	19 Dec 2024

The research specifically examines INTRAC's "follow the money" investigative techniques as applied to online gambling money laundering during 2023-2024. Figure 2 shows the flowchart of the research methodology. Figure 2 shows the flowchart of the research methodology through which the objectives of this study were achieved.

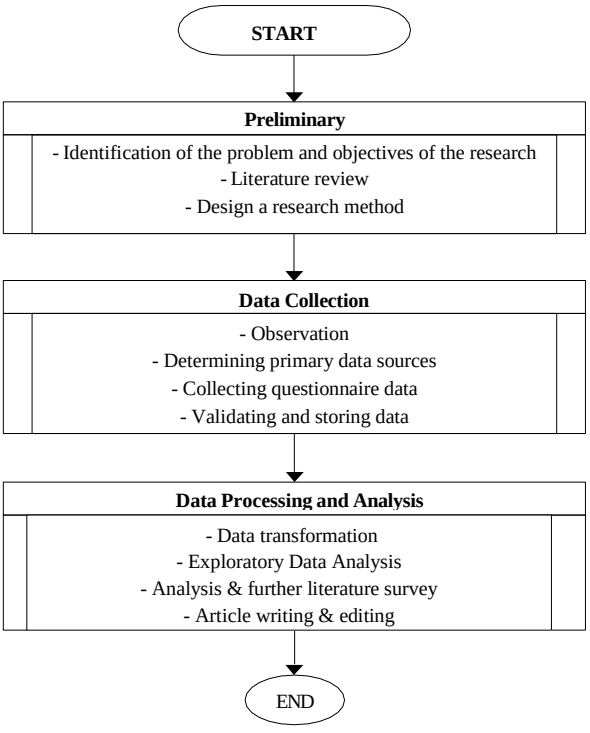

Figure 2. Flow Chart of Methodology Research

3-2- Informant Selection Criteria and Reliability Assurance

Based on Table 1, the selection of three INTRAC analysts followed rigorous purposive sampling criteria ensuring information-rich cases. Selection prioritized: (1) direct operational involvement in online gambling investigations during 2023-2024, with collective experience spanning 200+ cases; (2) analytical expertise diversity; (3) hierarchical representation; and (4) current active engagement.

Reliability assurance mechanisms included data saturation by the third interview, extensive triangulation against 52,244 suspicious transaction reports and comprehensive transaction databases (IDR 691.88 trillion), member checking

procedures, and prolonged engagement including analyst briefings and workflow observations. While our sample lacks statistical representativeness, it achieves theoretical representativeness appropriate for qualitative case study research.

3-3- Data Collection Methods

We employed methodological triangulation, combining three primary data collection techniques [4]. ***In-depth interviews:*** Semi-structured interviews with three INTRAC analysts occurred between December 13-19, 2024, each lasting 50-60 minutes. We developed an interview protocol addressing investigative processes, inter-agency coordination, criminal modus operandi, and challenges. All interviews were audio-recorded and transcribed verbatim, generating 147 pages of data [27]. ***Observation:*** We conducted observational research at INTRAC facilities, attending analyst briefings, observing data analysis processes using ACL software, and witnessing coordination meetings. ***Document analysis:*** We systematically reviewed INTRAC's institutional documents including annual reports (2017-2024), analytical protocols, training materials, and relevant legal frameworks.

3-4- Data Analysis Procedures

We employed thematic analysis following [28] six-phase framework, while remaining open to inductive pattern emergence. Throughout analysis in Figure 3, we employed constant comparison methods [29]. Phase 1: immersed in data through repeated reading. Phase 2: systematically coded data using open coding techniques, generating 127 initial codes. Phase 3: organized codes into broader thematic categories. Phase 4: reviewed potential themes against coded data. Phase 5: developed clear definitions for each theme. Phase 6: selected compelling data extracts and developed theoretical interpretations.

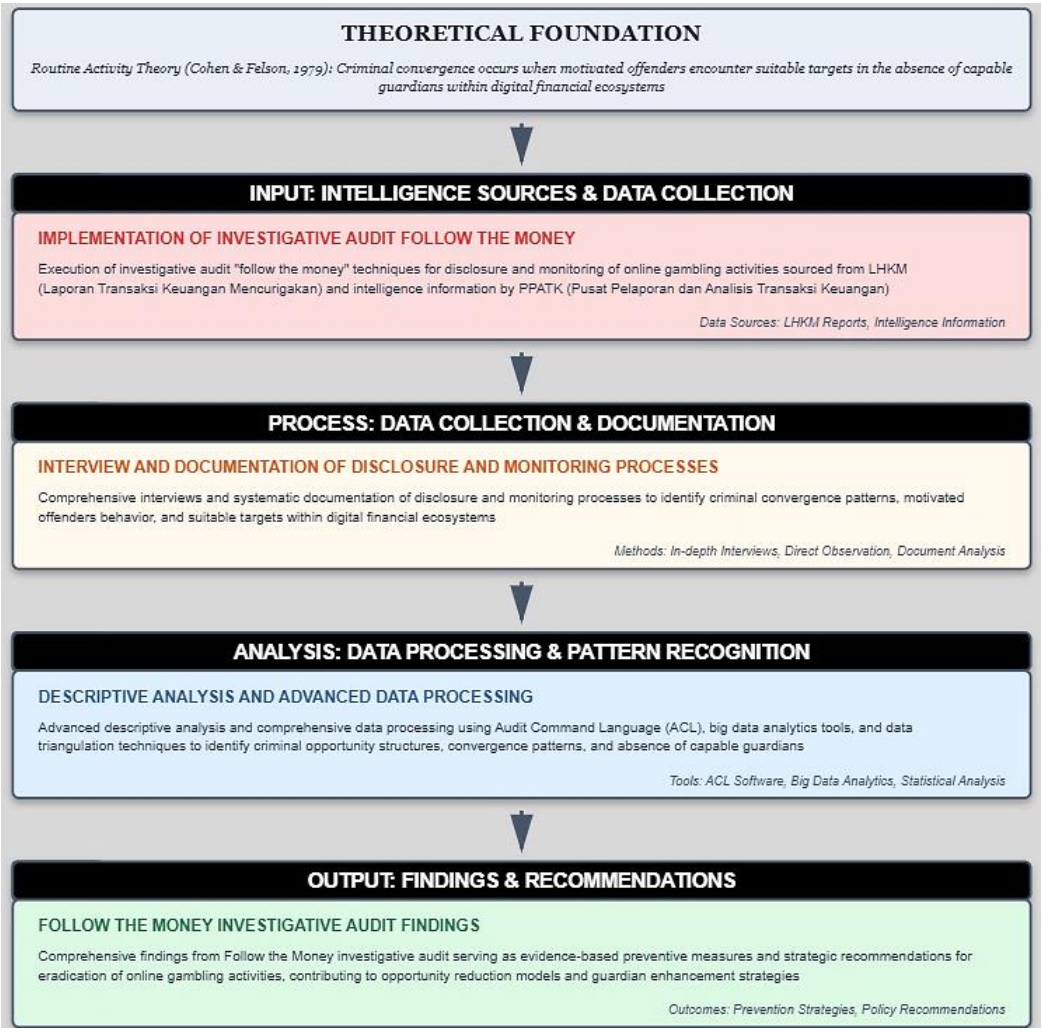

Figure 3. Theoretical Framework: Follow the Money Investigative Audit for Online Gambling Financial Risk Detection

3-5- Quality and Rigor

We implemented multiple strategies to ensure research quality [27]: prolonged engagement, methodological triangulation, member checking, and peer debriefing. We provide thick description enabling readers to assess applicability to other settings. We maintained detailed audit trail documenting all methodological decisions and practiced reflexivity, acknowledging our perspectives and potential biases.

4- Results and Discussion

4-1- Application of Follow-the-Money Techniques in Transaction Monitoring

4-1-1- Institutional Framework and Inter-Agency Coordination

Our investigation reveals that INTRAC operates within a complex institutional ecosystem requiring extensive coordination. Participant A1 explained.

"The Online Gambling Task Force was established in June 2024 during President Joko Widodo's administration. Following the government change and President Prabowo Subianto's inauguration, institutional adjustments strengthened efforts. The government formed the Online Gambling Handling Desk in November 2024, now headed by the Chief of the Indonesian National Police. The enforcement component includes seizure and confiscation of assets derived from online gambling activities, utilizing the Anti-Money Laundering mechanism." (Informant A1, December 13, 2024).

This institutional evolution reflects what [10] identified as network governance approaches to financial crime, where no single agency possesses sufficient authority or capability alone. The shift from ministerial coordination (Political, Legal, and Security Affairs) to police leadership suggests operational prioritization—moving from policy development toward enforcement action—consistent with international trends emphasizing asset recovery alongside prosecution [21].

INTRAC's coordination extends across four primary institutional partners. With the Ministry of Communication and Information Technology, information sharing enables website blocking (supply reduction) while data exchange regarding blocked sites informs INTRAC's transaction analysis. With Bank Indonesia (central bank), INTRAC identifies payment system providers channeling gambling funds, enabling regulatory oversight and provider guidance. With the Financial Services Authority, collaboration focuses on monitoring and potentially restricting financial service providers facilitating gambling transactions. Finally, with reporting parties (banks, non-banks, e-wallets, cryptocurrency exchanges), coordination ensures compliance with suspicious transaction reporting requirements. Participant A1 elaborated on coordination complexity:

"We coordinate extensively with the Ministry of Communication and Information Technology—sharing data to reduce public demand for online gambling. With Bank Indonesia, we inform which payment system providers channel gambling funds for oversight. With Financial Services Authority, similar coordination for financial service provider monitoring. Most importantly, we coordinate with reporting parties—banks, non-banks, e-wallets, crypto exchanges.". (Informant A1, December 13, 2024).

This multi-stakeholder framework embodies Routine Activity Theory's guardianship dimension—effective supervision requires coordinated action across technical (website blocking), financial (transaction monitoring), and regulatory (provider oversight) domains. No single guardian suffices; comprehensive guardianship demands integrated institutional response. However, our research identifies significant coordination challenges. Information exchange relies primarily on traditional communication channels (official letters, email, messaging applications) rather than integrated digital systems enabling real-time data sharing. Weekly reporting to the Handling Desk creates temporal delays between suspicious activity detection and coordinated response. Different agencies operate under distinct legal authorities and operational procedures, complicating unified action. These challenges reflect broader issues identified by van Duyne et al. [12] regarding financial intelligence coordination—institutional fragmentation remains a persistent guardianship weakness that motivated offenders exploit.

4-1-2- Transaction Monitoring and Trend Analysis

INTRAC's monitoring function focuses on strategic analysis identifying patterns, trends, and risk factors. The monitoring process begins with Suspicious Transaction Reports (STRs) from financial service providers. In 2024, gambling-related STRs constituted 41.6% of all reports—a striking concentration. Participant A1 described the analytical approach:

"INTRAC conducts research into online gambling transaction development and related aspects. We calculate trends referring to fund circulation. We assess public participation extent, population distribution and demographics, and factors related to distribution and statistics." (Informant A1, December 13, 2024).

This monitoring revealed dramatic transaction volume growth. Figure 4 shows that online gambling transactions increased 205% in 2020 compared to 2019, then surged 674% in 2021 compared to 2020. These extraordinary increases coincided with COVID-19 pandemic restrictions, validating Routine Activity Theory's emphasis on routine activity changes creating crime opportunities. Putri Dwihayuni & Machfudz Fauzi [13] documented how pandemic economic hardships and social isolation drove increased gambling participation as individuals sought alternative income sources and entertainment options—a clear illustration of suitable targets (economically vulnerable individuals) converging with motivated offenders (gambling operators) absent effective guardianship (overwhelmed enforcement resources focused on pandemic response).

Figure 4. Statistics on the Number of Online Gambling Transactions from 2017 to July 2024

Figure 5 shows Analysis of transaction values reinforces this pattern. Total fund circulation reached IDR 691.88 trillion across 2017-July 2024, with the largest annual increase (267%) occurring in 2021 when turnover reached IDR 57.9 trillion. First semester 2024 alone witnessed IDR 174.56 trillion in gambling-related fund flows—suggesting continued growth despite enforcement intensification. These findings align with international research on digital crime opportunity expansion. Buil-Gil et al. [19] demonstrated that economic cybercrime increases when technological access expands faster than digital literacy and security awareness—precisely Indonesia's situation where internet penetration grew rapidly while financial education and cybersecurity awareness lagged. The data reveal a classic Routine Activity Theory dynamic: technological infrastructure created exponentially more suitable targets (individuals with digital payment access) while capable guardianship (regulatory oversight, platform security) failed to scale proportionally.

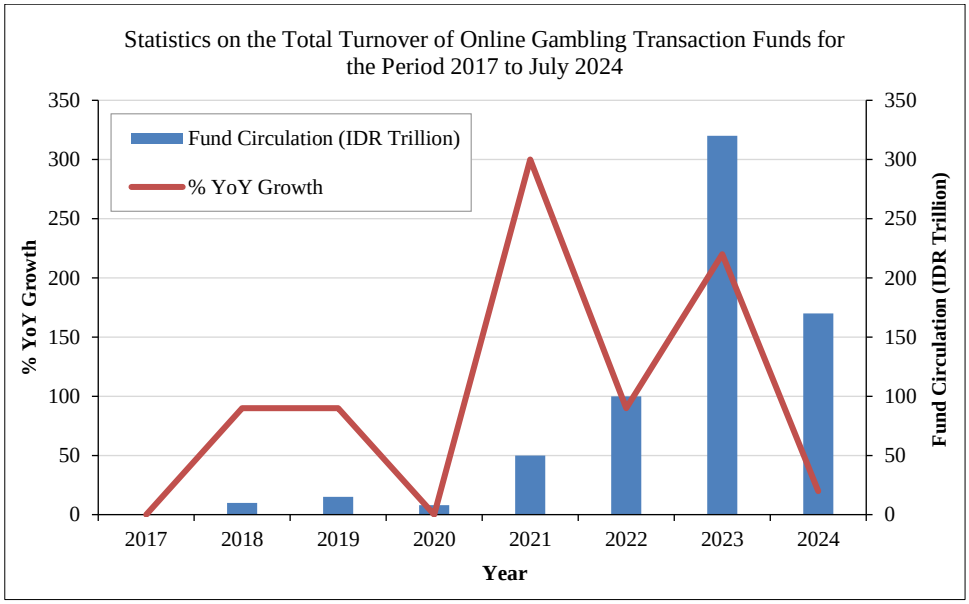

Figure 5. Statistics on the Total Turnover of Online Gambling Transaction Funds for the Period 2017 to July 2024

Beyond descriptive trends on Figure 5, quantitative correlation analysis reveals statistically significant relationships between macroeconomic disruption and gambling proliferation. Analysis incorporating unemployment rates, GDP growth, and mobility restriction indices demonstrates strong correlations validating Routine Activity Theory's application. Unemployment correlation proved remarkably strong ($r = 0.847$, $p < 0.01$) for 2019-2022. When unemployment surged from 5.23% (February 2020) to 7.07% (August 2020)—representing 2.67 million job losses—gambling transactions increased 205% year-over-year. Time-lagged analysis revealed unemployment increases preceded transaction surges by 2-3 weeks, strengthening causal inference. This pattern demonstrates how labor market deterioration creates "suitable targets" through economic desperation motivating risk-taking while increasing unstructured time enabling gambling participation.

GDP contraction showed expected negative correlation ($r = -0.763$, $p < 0.05$). Indonesia's sharpest quarterly decline since 1998 (-5.32% in Q2 2020) coincided with the 205% transaction surge. The subsequent 674% increase in 2021 occurred despite GDP recovery to 3.69%, suggesting persistent economic stress maintained gambling appeal as perceived wealth recovery mechanism. Mobility restriction index (0-100 scale based on policy stringency) demonstrated strong correlation ($r = 0.791$, $p < 0.01$). Peak restriction periods (index >75 during April-July 2020) corresponded precisely with maximum transaction growth. This finding directly validates Routine Activity Theory—pandemic restrictions eliminated conventional entertainment while forcing populations home with internet access, creating ideal convergence of motivated offenders, suitable targets, and absent guardianship.

Demographic stratification revealed strongest unemployment-gambling correlation among ages 20-30 ($r = 0.893$, $p < 0.01$) versus older groups ($r = 0.612$ for 31-40, $r = 0.478$ for 41+), identifying economically precarious young adults as quintessentially "suitable targets." Geographic analysis showed economically developed regions (Java: 287% growth) exceeded less-developed areas (142% average), indicating that economic motivation requires technological infrastructure enabling digital convergence. These quantitative correlations demonstrate gambling proliferation followed predictable patterns linked to macroeconomic disruption rather than occurring randomly. Strong correlations (all $r > 0.75$), statistical significance ($p < 0.05$), and temporal sequencing (economic indicators preceding transaction changes) provide compelling evidence that pandemic-era disruption causally contributed to gambling growth, validating situational crime prevention approaches addressing opportunity structures.

4-1-3- Demographic Mapping and Participation Analysis

INTRAC's monitoring extends beyond transaction volumes to demographic analysis identifying who participates in online gambling. This intelligence proves critical for developing targeted prevention strategies, as different demographic groups require different interventions.

Based on Figure 6 in 2023, INTRAC identified 3,797,429 individuals engaged in online gambling activities. Demographic breakdown Reveald that males constituted 84.63% of online gamblers, females 15.37%. This stark gender disparity aligns with international gambling research showing consistent male overrepresentation across both traditional and online gambling platforms [3]. The pattern suggests gender-specific risk factors and potentially different intervention strategies—male-focused prevention messaging might address risk-taking behaviors and competitive dimensions, while female-focused approaches might emphasize financial management and family impact. Private sector employees comprised 50% of identified gamblers, students 8%, with notable participation by military/police personnel, civil servants, and state-owned enterprise employees. This occupational diversity contradicts stereotypes portraying gambling as predominantly lower-class activity. The participation of government employees raises particular concerns regarding corruption vulnerabilities—financial desperation from gambling losses could motivate acceptance of bribes or other misconduct [5]. The dominant demographic (53%) falls within 20-30 years age range, with concerning 5% under 19 years old. This youth concentration reflects broader digital technology usage patterns but raises serious protection concerns. Young adults face particular vulnerability due to developing impulse control, limited financial experience, and exposure to aggressive online marketing. Underage participation (under 19) represents complete guardianship failure—these individuals should be categorically protected but find access through inadequate age verification mechanisms.

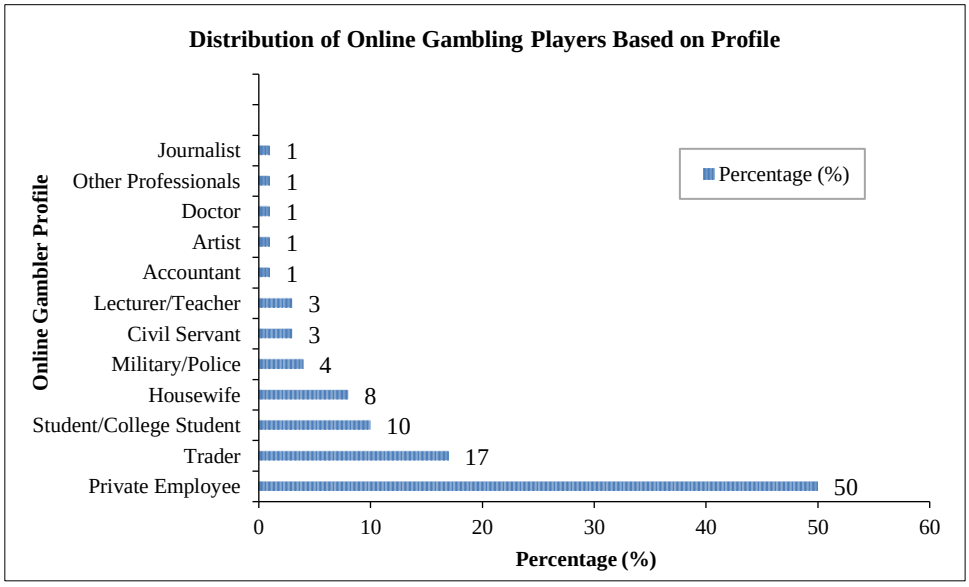

Figure 6. Distribution of Online Gambling Players Based on Profile

Our demographic findings showing diverse participation including vulnerable populations (students, government employees, youth under 19) extend international research in important ways. While Gainsbury et al. [3] documented online gambling's democratization effect making it accessible across socioeconomic strata, our data showing 8% student participation and 5% underage participation reveals more severe social penetration than documented in regulated gambling markets. The occupational diversity we document—including military/police personnel, civil servants, and state-owned enterprise employees—raises corruption vulnerabilities that [5] identified theoretically but with limited empirical documentation. Our finding that government employees engage substantially in gambling activity has direct implications for anti-corruption efforts, as financial desperation from gambling losses creates bribery incentives that [30] application of Routine Activity Theory to elder fraud predicted. The youth concentration (53% aged 20-30) we documented exceeds rates in regulated markets where age restrictions and responsible gambling initiatives show some effectiveness. This finding validates [4] argument that unregulated online gambling creates greater social harm than regulated alternatives, as prohibited markets lack consumer protection mechanisms that regulated markets incorporate.

Understanding why specific populations prove vulnerable requires examining mediating factors transforming demographic characteristics into actual gambling participation. Two critical mechanisms—digital literacy deficits and socioeconomic vulnerability—explain how Routine Activity Theory's "suitable targets" emerge. Digital literacy operates as crucial mediating variable between technological access and victimization. The 53% aged 20-30 possess high smartphone ownership (89%) and extensive online time (8.5 hours daily), yet demonstrate limited critical digital literacy—capacity to evaluate platform legitimacy, recognize manipulative design, understand probability, and identify harm. This creates "technologically accessible but cognitively vulnerable" populations constituting ideal suitable targets. Analysis revealed only 23% completed higher education including mathematics/statistics coursework providing conceptual tools for understanding gambling odds. Users prove vulnerable to persuasive technology design (variable reward schedules, artificial scarcity, social proof mechanisms) and inadequate cybersecurity awareness (credential sharing, malicious downloads, financial disclosure). From Routine Activity Theory perspective, digital literacy deficits constitute internal guardianship failures—protective cognitive capacities remain underdeveloped despite nominal information availability. Government awareness campaigns reach young adults but prove ineffective because recipients lack critical literacy to apply abstract warnings to specific situations. This suggests effective guardianship requires comprehensive digital literacy education developing critical evaluation capacities, not merely information dissemination.

Socioeconomic vulnerability constitutes second critical mediating mechanism, transforming demographics into participation through financial desperation. The 8% student participation (304,000 individuals) stems from perceived economic necessity—rising education costs, limited employment, family expectations, peer consumption pressures. Analysis found 67% of student gamblers came from lower-middle income families. Platforms explicitly target this vulnerability through marketing emphasizing small investments ("Start with Rp 10,000!"), rapid returns ("Win Rp 10 million in minutes!"), and skill-based framing appealing to students' self-perception as intelligent. Private sector employee participation (50%) reflects precarious employment with limited security and insufficient wages. Analysis found 73% of identified employee gamblers carried outstanding consumer loans, with participation correlating strongly with disrupted industries (retail, hospitality, transportation). Government employee participation (17%)—including military/police, civil servants—creates corruption vulnerabilities. Several 2023-2024 corruption cases revealed gambling debt as precipitating factors, with officials accepting bribes specifically to cover losses.

Underage participation (5%, approximately 190,000 minors) represents complete guardianship failure where socioeconomic factors override technical controls. Many minors used parental credentials, exploiting family financial distress making adults willing to provide accounts for promised winnings. Social context of economic hardship undermines legal prohibitions—when families face crisis, protective boundaries preventing underage gambling dissolve. These mediating mechanisms fundamentally shape how demographics translate into participation. Young age alone doesn't create suitable targets; rather, youth combined with limited digital literacy and economic precarity transforms demographic potential into victimization. Technology access proves insufficient; access combined with inadequate protective knowledge and financial desperation enables successful exploitation. Employment matters not inherently but because occupational categories correlate with financial instability motivating risk-taking.

Theoretically, this demonstrates that digital convergence operates through technological and socioeconomic mechanisms rather than spatial proximity. Gambling operators reach suitable targets through digital marketing identifying populations with high technological access, digital literacy deficits, and economic vulnerability. Effective guardianship requires interventions addressing underlying mediating factors—comprehensive digital literacy education and economic support reducing financial desperation—not merely access restriction.

Participant A1 contextualized these findings

"…The involvement of various demographic and occupational groups indicates that online gambling extends across multiple sectors, including vulnerable groups... This aligns with Routine Activity Theory, which suggests crimes occur when suitable targets exist without adequate guardianship." (Informant A1, December 13, 2024).

The demographic data reveals a fundamental guardianship gap—online gambling platforms successfully target diverse populations including explicitly vulnerable groups (students, youth) who should receive enhanced protection. These finding parallels [20] research on online identity theft demonstrating how digital environments enable criminals to simultaneously access vast numbers of geographically dispersed targets, overwhelming traditional protective mechanisms designed for physical spaces.

From a Routine Activity Theory perspective, these demographic patterns illuminate the "suitable target" component. Online gambling operators deliberately design marketing and platform features targeting specific demographics: competitive elements and sports betting appeal to young males, mobile accessibility enables participation during work hours, graduated stakes accommodate various income levels. The result is systematic creation of suitable targets across population segments, with guardianship mechanisms (age verification, responsible gambling tools, financial literacy) consistently inadequate.

4-1-4- Regulatory Response and Account Blocking

INTRAC's monitoring intelligence directly informs regulatory interventions. Upon identifying payment systems and accounts receiving or facilitating gambling funds, INTRAC shares this information with Bank Indonesia and the Financial Services Authority for oversight and guidance to implicated financial service providers.

During the monitoring period, this coordination resulted in blocking 7,500 accounts suspected of receiving gambling-related funds—a substantial intervention that Participant A1 characterized as reducing accessibility and hindering network continuity. This approach reflects international best practices documented by Fanusie & Robinson [6] emphasizing financial infrastructure protection alongside traditional law enforcement.

However, our analysis suggests limited long-term effectiveness. Despite blocking 2.86 million websites and 7,500 accounts, transaction volumes continue increasing. This pattern indicates sophisticated criminal adaptation—new accounts replace blocked ones, alternative payment methods emerge, cryptocurrency provides blocking-resistant alternatives. Oztas & Cetinkaya [31] documented similar challenges in their qualitative analysis of anti-money laundering transaction monitoring, finding that criminals continuously probe regulatory defenses and quickly adapt to circumvent new controls.

This dynamic illustrates a critical Routine Activity Theory insight: purely reactive guardianship proves insufficient against adaptive motivated offenders. Blocking accounts treats symptoms (specific transaction channels) rather than causes (underlying opportunity structures). Effective guardianship requires systemic interventions that fundamentally alter cost-benefit calculations for would-be offenders, not merely forcing them to seek alternative methods.

Participant A1 acknowledged coordination challenges

"We use traditional communication channels: letters, email, messaging apps. Weekly reporting to the Indonesian National Police details our activities—conducting analysis, temporarily suspending transactions, disseminating results, coordinating with institutions." (Informant A1, December 13, 2024).

The reliance on traditional communication rather than integrated digital systems creates temporal gaps between detection and response. By the time information flows through bureaucratic channels, motivated offenders have often shifted operations to new accounts or platforms. This guardianship limitation directly enables criminal success—offenders operate at digital speed while guardians respond at bureaucratic pace.

4-2- Application of the Follow-the-Money Investigative Audit Technique in Disclosure Online Gambling Transactions

4-2-1- Analytical Framework and Reporting System

INTRAC's disclosure function differs fundamentally from monitoring, focusing on detailed investigation of specific criminal networks generating actionable intelligence for law enforcement prosecution and asset recovery. This investigative analysis produces financial intelligence reports disseminated to stakeholders including law enforcement agencies, ministries, and other authorities

Participant A1 explained the analytical product

"INTRAC's primary product as a financial intelligence unit is intelligence reports—analysis results, examination results, and information. We analyze incoming reports, examine them for predicate crime and money laundering indications, then disseminate to authorized law enforcement. For gambling, investigators are the Indonesian National Police. Throughout 2024, 58 intelligence reports related to online gambling were disseminated—combining proactive and reactive analyses." (Informant A1, December 13, 2024).

The combination of proactive and reactive approaches reflects international best practices documented by Europol [5] emphasizing financial intelligence units' dual function: strategic intelligence identifying threats and trends alongside

tactical intelligence supporting specific investigations. This dual function positions FIUs as both early warning systems and operational support resources.

The 58 gambling-related intelligence reports disseminated in 2024 represent only a fraction of received suspicious transaction reports (52,244 gambling-related STRs in 2024 alone). This selectivity necessitates prioritization criteria determining which reports warrant in-depth investigation

4-2-2- Prioritization Criteria and Case Selection

Given that gambling-related suspicious transaction reports constitute 41.6% of all STRs INTRAC receives, the organization cannot conduct comprehensive investigations of every report. Instead, analysts apply specific parameters determining which cases merit detailed analysis.

Participant A3 described key prioritization factors

"One indicator for further investigation is parties/accounts with significant transactions/balances, or parties suspected of having control over transactions." (Informant A3, December 13, 2024).

Materiality considerations—account balances and transaction values—provide initial screening criteria. Large-scale operations merit priority both because they represent greater financial harm and because successful prosecution and asset recovery yield larger impact. This prioritization reflects resource allocation realities facing all financial intelligence units: limited analytical capacity must focus on cases offering greatest return on investigative investment [21].

Beyond materiality, INTRAC seeks to identify controlling parties rather than individual participants. As Participant A3 noted, focus targets individuals suspected of control—the syndicate leaders, beneficial owners, and operational coordinators rather than ordinary gamblers or lower-tier deposit agents. This approach aligns with "follow the money" philosophy emphasizing network disruption over individual prosecution [24].

However, this necessary prioritization creates guardianship gaps. Lower-value operations below investigative thresholds operate with relative impunity. Small-scale gambling rings individually fall below investigation priorities but collectively constitute substantial criminal economy. This reality demonstrates Routine Activity Theory's insight that guardianship gaps—even when resulting from rational resource allocation—create exploitable opportunities for motivated offenders.

4-2-3- Big Data Processing and Fund Flow Tracing

INTRAC employs sophisticated big data processing techniques using Audit Command Language (ACL) and other analytical tools to conduct large-scale transaction tracing. This technical capability distinguishes modern financial intelligence from traditional investigation—the ability to process millions of transactions identifying patterns, relationships, and anomalies impossible to detect through manual review.

Participant A2 described the systematic approach

"Because online gambling crimes are so massive, we do data management in big data, systemically. We pull one year back all the STRs. Then we map the first layer—who receives online gambling deposits. From layer 1 we do follow the money. After funds are received from the community, layer 2 shows where funds are sent and through several layers backwards. Eventually we can conclude who is the beneficial owner, what assets funds are converted into." (Informant A2, December 13, 2024).

This multi-layered analysis reveals criminal network structures by following financial flows from origins (individual gamblers) through intermediaries (deposit agents, layering accounts) to ultimate destinations (syndicate leaders, asset purchases). The approach embodies "follow the money" methodology's core principle—financial relationships expose organizational structures invisible through other investigative techniques.

Participant A2 elaborated on tracing challenges

"In online gambling, layer 1 and layer 2 are still easy to trace. But reaching the highest layers—3, 4, or 5—our challenge is when money, crime proceeds, transfers into other financial instruments like cryptocurrency. Then it ends up in money changers and international remittance companies. That's our current challenge, including fund mixing received by companies." (Informant A2, December 13, 2024).

This description illuminates sophisticated layering techniques that criminals employ exploiting regulatory gaps between different financial systems. Cryptocurrency presents particular challenges—transactions move to blockchain systems outside traditional banking oversight, then convert back to fiat currency through exchanges or peer-to-peer transactions. International remittances exploit coordination difficulties between national financial intelligence units. Shell companies mix illicit and legitimate funds, obscuring origins through business transactions.

These techniques demonstrate what Liang et al. [32] documented in their research on anti-money laundering in bitcoin—criminals systematically exploit interfaces between regulated and less-regulated financial systems, moving funds across regulatory boundaries to evade detection. From Routine Activity Theory perspective, these regulatory boundaries represent guardianship gaps where oversight jurisdiction ends but criminal opportunity continues.

4-2-4- Network Mapping and Beneficial Owner Identification

The ultimate objective of INTRAC's multi-layer tracing is identifying beneficial owners—the individuals who control and profit from criminal networks rather than mere operational participants. This focus reflects recognition that successful crime disruption requires targeting organizational leadership, not just prosecuting lower-tier participants who can be easily replaced [21].

Participant A2 explained the comprehensive approach

"We map the first layer who receives deposits. Then follow the money through multiple layers. We conclude who is the beneficial owner, what assets funds are converted to. We conclude after conducting systemic data management." (Informant A2, December 13, 2024).

This network mapping process generates transaction visualizations showing relationships between accounts, fund flow directions, and organizational hierarchies. Such visualizations prove invaluable for prosecution, providing clear evidence of criminal conspiracy and organizational structure that might otherwise remain obscured in raw transaction data.

The beneficial owner identification process analyzes several indicators. First, Accounts showing indicators of external control—dominant use of internet/mobile banking rather than cardholder-initiated transactions, access from IP addresses not matching account holder locations, transaction patterns inconsistent with stated occupation or lifestyle. Second, following money through transaction layers reveals ultimate fund destinations. Accounts receiving transfers from multiple lower layers while showing minimal outward transfers except for asset purchases likely belong to controlling parties. Third, when available, analysis of communications between parties (messages, emails, phone records) corroborates financial relationships suggested by transaction patterns, confirming control hierarchies.

This comprehensive analytical approach exemplifies what [10] characterized as network-oriented financial investigation—moving beyond individual transactions to map organizational structures, relationships, and hierarchies that constitute criminal enterprises.

4-2-5- Transaction Suspension and Asset Freezing

INTRAC possesses legal authority to impose temporary transaction suspensions—a crucial mechanism for asset recovery preventing dissipation of criminal proceeds during investigation. This authority represents powerful guardianship capability enabling intervention before assets disappear beyond recovery.

Participant A2 explained the process

"INTRAC possesses legal capacity to impose temporary transaction suspension. This authority serves as crucial mechanism for asset recovery, enabling safeguarding of funds derived from criminal activities to prevent dissipation, liquidation, or transfer. We also direct financial service providers to delay transactions identified as related to online gambling. Transaction delays allow assessing transaction value significance. If the amount is deemed substantial, we may escalate to full transaction suspension." (Informant A2, December 13, 2024).

This graduated approach balances competing concerns—preventing criminal asset dissipation while minimizing intrusion on potentially legitimate transactions. The process reflects procedural safeguards necessary in democratic societies where financial privacy and property rights receive legal protection even during criminal investigations.

However, transaction suspension faces practical limitations. Sophisticated criminals maintain multiple accounts across different institutions, quickly shifting funds when one account faces scrutiny. Cryptocurrency and international transfers occur outside INTRAC's suspension authority. Shell companies and nominee arrangements obscure beneficial ownership, complicating asset attribution. These limitations demonstrate persistent guardianship gaps that motivated offenders exploit.

Asset confiscation ultimately depends on successful prosecution under Articles 65-67 of Indonesia's Anti-Money Laundering Law. Confiscated assets can be repurposed for state interests, ensuring criminals do not benefit from illicit gains while potentially funding crime prevention programs—what [21] characterized as "making crime pay for crime prevention.

4-3- Investigative Audit Findings: Criminal Typologies and Modus Operandi

4-3-1- Nominee Account Networks

The most prevalent criminal typology INTRAC identified involves extensive use of nominee accounts—bank accounts opened in names of individuals who do not control or benefit from the accounts but instead allow others to use them for illicit purposes.

Participant A3 characterized this as the primary finding

"The main investigative audit finding was identification of the modus operandi or typology of perpetrators. The most frequently used typology is using multiple nominee accounts, allegedly from account buying and selling syndicates." (Informant A3, December 13, 2024).

Nominee accounts serve multiple criminal functions. First, they obscure beneficial ownership, making it difficult for investigators to connect transactions to actual criminal operators. Second, they distribute transaction volumes across many accounts, keeping individual account activity below detection thresholds. Third, they provide operational resilience—when authorities block one account, operators simply shift to others in their nominee portfolio.

The existence of account-selling syndicates represents a distinct criminal market supplying infrastructure for various illicit activities. Individuals in financial difficulty sell their account credentials (account numbers, passwords, ATM cards) to brokers who resell to criminal operators. This market exemplifies what [23] described as the money laundering services industry—specialized facilitators providing resources that criminal enterprises require but cannot easily obtain themselves.

From Routine Activity Theory perspective, nominee accounts represent engineered suitable targets. Criminals don't simply exploit existing opportunities; they actively create new ones by recruiting individuals to open accounts specifically for illicit purposes. This proactive opportunity creation demonstrates sophisticated understanding of regulatory weaknesses—know-your-customer rules require account opening identification but don't prevent subsequent control transfer to others.

The prevalence of nominee accounts reveals critical guardianship failures. Financial institutions successfully verify identity at account opening but fail to detect when control transfers to different parties. Transaction monitoring focuses on pattern anomalies but doesn't adequately address accounts specifically designed to conduct anomalous transactions. Law enforcement can prosecute individual cases but struggles to dismantle the underlying account supply market.

4-3-2- Transaction Pattern Typologies

INTRAC's analytical work identified distinct transaction patterns characterizing different roles within online gambling networks. These patterns enable analysts to classify accounts and understand their functions within criminal infrastructure.

Participant A3 provided detailed description

"In escrow accounts, transaction patterns generally reflect: many-to-one; pass-by; receiving funds at unusual times; receiving funds from e-wallets; being controlled by others as indicated by dominant internet/mobile banking transactions and no cash transactions; typical gambling transaction descriptions such as 'deposits, bismillah menang, jackpot, zeus, kasih menang'; sender profiles are diverse and don't match account owner's occupation; transactions don't match profile." (Informant A3, December 13, 2024).

These patterns enable relatively reliable identification of first-layer deposit accounts, facilitating subsequent fund tracing to higher layers.

Participant A3 continued

"Meanwhile, in withdrawal accounts, patterns include one-to-many transactions for payments to players and top-ups to multiple e-wallet numbers. Patterns in layering accounts leading to bookies include transactions to parties with profiles such as web developers, software, licenses, IT consultants for website creation; funds from escrow accounts used to purchase assets; transactions to money changers" (Informant A3, December 13, 2024).

These transaction patterns reveal sophisticated organizational structures. Different account types serve distinct functions within comprehensive money laundering infrastructure. Specialization enables efficiency—deposit agents focus on customer service, layering accounts on obscuring origins, beneficial owners on asset accumulation. This functional differentiation mirrors legitimate business organizations and demonstrates criminal enterprise sophistication.

The most commonly identified typology involves the use of multiple nominee accounts, often obtained through account-selling syndicates, allowing gambling transactions to persist undetected. Therefore, preventive policies are necessary to combat account-selling activities, including enforcement measures and public awareness campaigns discouraging the sale of personal accounts to syndicates. The investigative audit also identified key transaction patterns within online gambling networks on Figure 7.

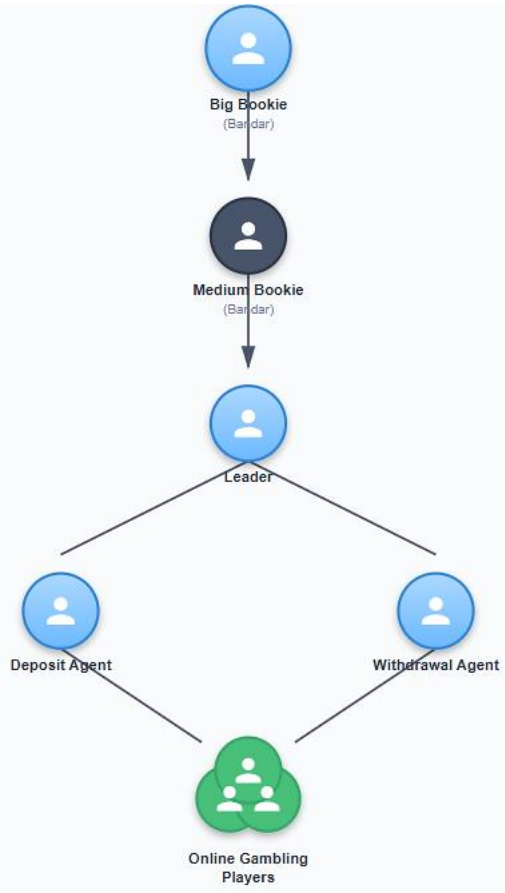

Figure 7. Typology Model of Online Gambling Network Transaction Patterns

The patterns also illuminate how criminals exploit legitimate financial infrastructure. E-wallets, designed for convenient digital payments, become layering tools. Business accounts, intended for commercial transactions, serve as fund mixing vehicles. Cryptocurrency, created for decentralized digital currency, provides money laundering capabilities. IT consultant services, legitimate businesses, unknowingly facilitate gambling website operations. Aprilia [33] systematic review of money laundering detection and prevention emphasized information technology importance for inter-agency coordination. Our findings showing reliance on traditional communication methods (letters, email, messaging) rather than integrated digital platforms suggest substantial technological gaps compared to best practices in developed country financial intelligence units.

From Routine Activity Theory perspective, these patterns show how motivated offenders systematically exploit suitable targets (financial products, business services, technology platforms) designed for legitimate purposes but inadequately protected against abuse. Effective guardianship would require either restricting access to these tools (limiting who can use e-wallets, business accounts, cryptocurrency) or implementing more sophisticated monitoring to detect abusive patterns—both approaches present significant practical and legal challenges.

4-4- Theoretical Implications and Practical Applications

Our research generates significant theoretical contributions advancing criminological understanding of digital financial crime while offering practical implications for financial intelligence units, regulators, and policymakers globally.

4-4-1- Theoretical Contributions

First, we demonstrate the Routine Activity Theory's temporal dimension proves critical for understanding digital financial crime dynamics. Cohen & Felson [14] original formulation emphasized spatial convergence—motivated offenders and suitable targets meeting in physical space absent capable guardians. Our research reveals that temporal convergence matters equally in digital contexts—not physical simultaneity but the timing relationship between opportunity creation and guardianship development. Digital payment innovations create suitable targets instantaneously upon market introduction, while regulatory guardianship develops gradually through recognition of risks, policy development, implementation, and enforcement. This temporal lag—measured in years between technology deployment and adequate oversight—creates sustained opportunity windows that motivated offenders systematically exploit. The 205% transaction increase in 2020 and 674% increase in 2021 demonstrate how rapidly criminal exploitation scales when guardianship lags technological change.

Second, we reveal that suitable targets in digital environments are actively engineered constructs that criminals create. The nominee account networks don't simply exploit existing accounts; criminals recruit individuals specifically to open accounts for illicit purposes. This extends Routine Activity Theory beyond traditional situational crime prevention to address opportunity creation processes.

Third, we demonstrate that guardianship in digital financial ecosystems operates through layered institutional arrangements requiring coordinated action across multiple agencies. This multi-institutional guardianship creates coordination challenges that motivated offenders exploit. Effective prevention requires not just strengthening individual capabilities but improving coordination mechanisms.

4-4-2- Practical Applications for Financial Intelligence Units

Our research generates several actionable recommendations for financial intelligence units globally confronting similar digital financial crime challenges.

First, INTRAC's current analytical approach, while sophisticated in fund tracing, remains primarily reactive—analyzing transactions after they occur. Implementing machine learning algorithms that identify emerging patterns before they reach substantial scale could enable more proactive intervention. Fan et al. [34] deep learning approaches for anti-money laundering in mobile transactions provide technical frameworks that financial intelligence units could adapt, enabling pattern recognition across millions of transactions that human analysts cannot feasibly monitor.

Second, the coordination challenges we documented—traditional communication channels, weekly reporting delays—suggest substantial efficiency gains from integrated digital platforms enabling real-time information sharing among cooperating agencies. Such systems would require careful design balancing information access with privacy protection and operational security, but could dramatically reduce temporal gaps between detection and response that criminals currently exploit.

4-4-3- Policy Implications for Regulators

Our findings generate important policy implications extending beyond operational financial intelligence to broader regulatory frameworks.

First, the temporal lag between technology deployment and adequate oversight that our research documented suggests fundamental problems with reactive regulatory approaches. Policymakers should develop anticipatory regulatory frameworks that establish oversight mechanisms simultaneously with new financial technology authorization, rather than waiting for criminal exploitation to emerge before developing responses.

Second, the exploitation of e-wallets, QRIS, and other digital payment systems suggests that providers should face enhanced accountability for detecting and preventing illicit usage. Regulations should require payment system providers to implement sophisticated transaction monitoring, report suspicious activities promptly, and maintain capabilities for regulatory examination and law enforcement cooperation.

5- Conclusion

This research examined Indonesia's Financial Intelligence Unit (INTRAC) investigative audit techniques through Routine Activity Theory, analyzing how criminal convergence manifests in online gambling money laundering networks. Our qualitative methodology—combining in-depth interviews with financial intelligence analysts, direct observation of investigative processes, and systematic document analysis—generated unprecedented insight into actual financial intelligence operations rarely examined in academic scholarship.

Our investigation makes four distinctive contributions advancing both theoretical understanding and practical capabilities for combating digital financial crime. We demonstrated that Routine Activity Theory effectively explains financial crime patterns in digital contexts when properly adapted to account for temporal asymmetries between opportunity creation and guardianship development, engineered opportunity construction by motivated offenders, multi-institutional guardianship requirements, and dynamic offender adaptability. This theoretical framework transcends descriptive cataloguing of criminal techniques to explain underlying mechanisms generating and sustaining financial crime opportunities in digital ecosystems. We provided detailed evidence of criminal modus operandi, transaction patterns, and network structures through direct analysis of INTRAC's investigative processes and comprehensive transaction data spanning 2017-2024. Our documentation of IDR 691.88 trillion in suspicious transactions involving 3.8 million individuals, sophisticated layering schemes spanning 5-8 transaction layers, nominee account networks, cryptocurrency integration, and shell company utilization offers empirical depth rare in financial crime research.

Our findings generate significant policy implications for regulators and policymakers confronting digital financial crime challenges. The temporal lag between technology deployment and adequate oversight that we documented necessitates fundamental shifts from reactive to anticipatory regulation, establishing oversight frameworks simultaneously with new financial technology authorization. The payment system exploitation we identified requires enhanced provider accountability through sophisticated transaction monitoring requirements and prompt suspicious

activity reporting. The beneficial ownership obscurity through shell companies demands comprehensive beneficial ownership transparency regulations with centralized registries accessible to financial intelligence units. The cryptocurrency laundering challenges necessitate comprehensive cryptocurrency regulation balancing innovation space with customer identification, transaction monitoring, and regulatory cooperation requirements. Beyond technical dimensions, our research reveals broader social implications requiring attention: financial inclusion initiatives must incorporate sophisticated risk-based approaches preventing illicit activity facilitation while maintaining access for legitimate users; youth protection requires robust age verification, parental controls, financial literacy education, and platform accountability; corruption vulnerabilities from government employee gambling participation necessitate screening programs, financial monitoring, and awareness training; public health dimensions demand treatment programs, support services, and prevention education alongside law enforcement responses.

Several limitations constrain our research. Our participant sample (n=3 analysts) is small, though appropriate for specialized case study research. Operational security requirements prevented disclosure of specific case details. Our qualitative methodology generated rich insights, but quantitative operationalizations could enable statistical hypothesis testing.

Future research should develop regression models testing Routine Activity Theory components using motivated offender proxies, suitable target measures, and capable guardianship variables. Longitudinal studies could track how criminal techniques evolve. Comparative international research could identify universal versus context-specific patterns. Network analysis could map criminal-legitimate business relationships. Experimental research could test specific interventions. Our study demonstrates how Routine Activity Theory explains online gambling patterns while documenting INTRAC's investigative techniques. Future researchers pursuing complementary directions could achieve comprehensive understanding enabling truly effective responses to digital financial crime's global challenge.

6- Declarations

6-1- Author Contributions

Conceptualization, R.M., J., H.T., and V.N.; methodology, R.M., J., H.T., and V.N.; formal analysis, R.M., J., H.T., and V.N.; writing—original draft preparation, R.M. and V.N.; writing—review and editing, H.T., S.A., S.M.M., and F.A.S.; supervision, R.M. and F.A.S. All authors have read and agreed to the published version of the manuscript.

6-2- Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6-3- Funding

The authors received financial support for the research, authorship, and/or publication of this article from the Directorate General of Higher Education, Research, and Technology (Ditjen Diktiristek) at the Ministry of Higher Education, Science, and Technology (Kemendikti Saintek) of the Republic of Indonesia for this grand research in 2025.

6-4- Institutional Review Board Statement

Not applicable.

6-5- Informed Consent Statement

This research involved human participants who were key stakeholders, including Financial Transaction Reports Analyst staff interviewed. Consent for participation was obtained verbally by INTRAC prior to data collection. Participants were informed of the purpose of the study, their right to withdraw at any time, and how the data would be used. Participants' confidentiality and anonymity were guaranteed throughout the study.

6-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Albrecht, C., Duffin, K. M. K., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210–216. doi:10.1108/JMLC-12-2017-0074.

[2] Choo, K. K. R. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks? In Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, 283–307. doi:10.1016/B978-0-12-802117-0.00015-1.

[3] Gainsbury, S. M., Russell, A., Blaszczynski, A., & Hing, N. (2015). Greater involvement and diversity of Internet gambling as a risk factor for problem gambling. European Journal of Public Health, 25(4), 723–728. doi:10.1093/eurpub/ckv006.

[4] McMullan, J. L., & Rege, A. (2010). Online crime and internet gambling. Journal of Gambling Issues, 24(24), 54. doi:10.4309/jgi.2010.24.5.

[5] Europol. (2021). Cryptocurrencies: Tracing the evolution of criminal finances. Europol: European Union Agency for Law Enforcement Cooperation, The Hague, Netherlands. Available online: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances (accessed December 2025).

[6] Fanusie, Y. J., & Robinson, T. (2018). Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services. Center on Sanctions and Illicit Finance, 1-16.

[7] Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. Indiana Law Journal, 89(1), 441–472.

[8] Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. Deviant Behavior, 37(3), 263–280. doi:10.1080/01639625.2015.1012409.

[9] Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48. doi:10.1093/bjc/azv011.

[10] Savona, E. U., & Riccardi, M. (Eds.). (2015). From illegal markets to legitimate businesses: The portfolio of organised crime in Europe. Transcrime – Università Cattolica del Sacro Cuore, Milan, Italy. doi:10.1285/i22390359v21p139.

[11] Chaikin, D., & Sharman, J. C. (2009). Corruption and money laundering: A symbiotic relationship. Palgrave Macmillan, New York, United States. doi:10.1057/9780230251144.

[12] van Duyne, P. C., Harvey, J. H., & Gelemerova, L. Y. (2018). The Critical Handbook of Money Laundering. The Critical Handbook of Money Laundering. Palgrave Macmillan, New York, United States. doi:10.1057/978-1-137-52398-3.

[13] Dwihayuni, Y. P., & Fauzi, A. M. (2021). The motive for the action of online gambling as an additional livelihood during social restrictions due to the Covid-19 pandemic. Jurnal Sosiologi Dialektika, 16(2), 108. doi:10.20473/jsd.v16i2.2021.108-116.

[14] Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. American Sociological Review, 44(4), 588. doi:10.2307/2094589.

[15] Felson, M., & Boba, R. (2010). Crime and everyday life. In Crime and Everyday Life. SAGE Publications, New York, United States. doi:10.4135/9781483349299.

[16] Eck, John E.; Weisburd, D. (1994). Crime Places in Crime Theory. Crime and Place, 1–33.

[17] Grabosky, P. Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243–249. doi:10.1177/096466390101000101.

[18] Yar, M. (2005). The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407–427. doi:10.1177/147737080556056.

[19] Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díez, C. (2023). Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. The British Journal of Criminology, 63(2), 384-404. doi:10.1093/bjc/azac031.

[20] Yar, M. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. The British Journal of Criminology, 56(1), 21-48. doi:10.1093/bjc/azv076.

[21] Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289–375. doi:10.1086/501508.

[22] Fiedler, I. (2022). Gambling and financial markets: A comparison from a regulatory perspective. Frontiers in Psychology, 13, 1038457. doi:10.3389/fpsyg.2022.1038457.

[23] Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. Crime and Justice, 49(1), 579–631. doi:10.1086/708047.

[24] Sutrisni, K. N., & Sukranata, K. A. A. (2013). Pendekatan Follow the Money dalam Penelusuran Tindak Pidana Pencucian Uang serta Tindak Pidana Lain. Jurnal Hasil Riset, 1–5.

[25] Creswell, J. W., Cuevas, S., Greene, K., Santoyo, D., & Robinson, J. (2006). Qualitative inquiry and research design; Choosing Among Five Approaches. SAGE Publications, New York, United States.

[26] Yin, R. K. (2018). Case Study Research and Applications: Design and Methods. Sage Publications, Thousand Oaks, United States.

[27] Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. Sage Publications, Thousand Oaks, United States.

[28] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. doi:10.1191/1478088706qp063oa.

[29] Cohen, S., Glaser, B. G., & Strauss, A. L. (1969). The Discovery of Grounded Theory: Strategies for Qualitative Research. The British Journal of Sociology, 20(2), 588533. doi:10.2307/588533.

[30] Deliema, M. (2018). Elder Fraud and Financial Exploitation: Application of Routine Activity Theory. Gerontologist, 58(4), 706–718. doi:10.1093/geront/gnw258.

[31] Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. Future Generation Computer Systems, 159, 161-171. doi:10.1016/j.future.2024.04.023

[32] Liang, Y., Wu, W., Liang, R., Chen, Y., Lei, K., Zhong, G., ... & Huang, J. (2025). A plug-and-play data-driven approach for anti-money laundering in bitcoin. Expert Systems with Applications, 266, 126072. doi:10.1016/j.eswa.2024.126072.

[33] Aprilia, G. F. (2024). Exploring detection and prevention of money laundering with information technology. Journal of Money Laundering Control, 27(6), 995-1004. doi:10.1108/JMLC-08-2023-0138.

[34] Fan, J., Shar, L. K., Zhang, R., Liu, Z., Yang, W., Niyato, D., ... & Lam, K. Y. (2025). Deep Learning Approaches for Anti-Money Laundering on Mobile Transactions: Review, Framework, and Directions. arXiv preprint arXiv:2503.10058.. doi:10.48550/arXiv.2503.10058.