Parallel Banking Through Fintechs: Regulatory Blind Spots, Tax Evasion and Money Laundering in Emerging Markets

Gustavo Henrique Rodrigues Pessoa *

Posted Date: 3 December 2025

doi: 10.20944/preprints202512.0420.v1

Keywords: Fintech; money laundering; parallel banking; payment institutions; regulatory arbitrage; AML/CFT; shadow banking; tax evasion; Brazil

 doi:10.20944/preprints202512.0420.v1

Article

Parallel Banking Through Fintechs: Regulatory Blind Spots, Tax Evasion and Money Laundering in Emerging Markets

Gustavo Henrique Rodrigues Pessoa

Fundação Getulio Vargas; gustavo.pessoa@fgv.edu.br

Abstract

This article examines how fintechs and payment institutions in emerging markets have been used as parallel banking infrastructures that facilitate tax evasion, large-scale money laundering and regulatory arbitrage. Focusing on Brazil, it analyzes recent high-profile investigations—such as the Carbono Oculto, Tank and Quasar operations—to show how criminal organizations exploited payment institutions, digital accounts and card schemes to move value outside the visibility of traditional banks and supervisory authorities. The study employs a qualitative, document-based approach, drawing on official reports, judicial decisions, supervisory guidance and financial intelligence materials to map the architecture of fintech-enabled illicit finance. The findings show that fintechs and payment institutions provided anonymity, opacity and transactional mobility through fragmented regulatory perimeters, lighter reporting requirements and gaps between financial, tax and AML/CFT oversight. These blind spots allowed parallel banking structures to operate at national scale while remaining formally within the legal financial system. The article contributes by proposing an integrated conceptual framework for understanding fintech-enabled parallel banking in emerging markets and by outlining policy recommendations to close supervisory gaps, align reporting obligations across institutions and strengthen cooperation between financial regulators, tax authorities and law-enforcement agencies.

Keywords: Fintech; money laundering; parallel banking; payment institutions; regulatory arbitrage; AML/CFT; shadow banking; tax evasion; Brazil

1. Introduction

In the past decade, fintechs and payment institutions have transformed the financial landscape across emerging markets. Designed to increase competition, reduce costs and promote financial inclusion, these entities now process trillions in digital payments and have become critical components of national payment systems. However, the rapid expansion of fintechs has outpaced the development of supervisory frameworks, creating blind spots in anti-money laundering (AML), financial intelligence and tax enforcement. These gaps have enabled the rise of *parallel banking infrastructures*—non-bank channels capable of performing functions traditionally associated with regulated banks, but with lower oversight, lighter reporting requirements and greater operational opacity.

Brazil's recent large-scale investigations revealed the full extent of this phenomenon. The 2025 Carbono Oculto operation uncovered fintechs that operated as shadow banks for criminal organizations, processing more than R$ 50 billion in transactions through omnibus accounts, fragmented wallets and non-traceable payment flows. The investigation exposed a network of shell companies, payment platforms, investment funds, holding structures and logistics operators acting collectively to evade taxes, launder money and disguise beneficial ownership. Similar findings emerged in the Tank, Quasar, Poço de Lobato and Cana Caiada operations, demonstrating that fiscal

 doi:10.20944/preprints202512.0420.v1

and financial crime had converged within fintech-enabled ecosystems characterized by mobility, anonymity and weak perimeter governance.

These developments point to a broader structural transformation in financial crime. Traditional AML frameworks were built around banks, which operate within well-defined supervisory perimeters. Fintechs, by contrast, rely on modular architectures, outsourced compliance, digital onboarding, embedded finance and multiparty data flows—all of which complicate traceability. In multiple jurisdictions, criminals leveraged payment institutions to bypass know-your-customer (KYC) controls, mix licit and illicit funds, fragment deposits, and move capital beyond the visibility of regulators.

The Brazilian case illustrates how regulatory fragmentation—between tax authorities, financial supervisors, AML units and sectoral regulators—amplifies these vulnerabilities. While banks are subject to extensive reporting obligations, fintechs historically operated under lighter requirements, including exemptions from comprehensive financial reporting to tax authorities. This disparity created opportunities for large-scale laundering and tax evasion, enabling criminal groups to embed parallel financial infrastructures within legitimate markets.

This article argues that fintech-enabled parallel banking represents one of the most significant emerging challenges for AML/CFT and financial regulation. By analysing Brazil's recent operations and connecting them to global evidence from FATF, IMF, BIS and FinCEN, the study offers an international framework for understanding how these schemes operate and provides policy recommendations to strengthen supervisory perimeters, harmonize reporting obligations and build integrated oversight architectures.

2. Background and Conceptual Framework

The rapid expansion of fintechs and payment institutions has fundamentally reshaped the architecture of financial intermediation. While these innovations increased efficiency and financial inclusion, they also created new vulnerabilities for anti-money laundering (AML) systems and tax enforcement. Traditional regulatory frameworks were designed for banks operating within clear institutional boundaries; fintechs, however, emerged as modular, technology-driven intermediaries capable of executing payments, holding funds, routing transactions and offering financial services without performing the functions of a traditional bank. This shift generated structural blind spots that criminal organizations learned to exploit.

At the core of these vulnerabilities is parallel banking—the use of non-bank financial entities to perform functions analogous to banking, such as accepting funds, transferring value, pooling deposits, providing liquidity and obscuring ownership. Parallel banking arises when non-bank institutions gain operational capabilities similar to banks but remain outside equivalent supervisory obligations. Fintechs and payment institutions, particularly in emerging markets, became vehicles for this phenomenon due to their lighter regulatory burdens, fragmented oversight and technological flexibility. These entities often rely on digital wallets, sub-accounts, multi-layered payment chains and outsourced compliance, all of which complicate AML monitoring and the identification of suspicious activity.

Another element shaping the conceptual framework is regulatory fragmentation. AML enforcement traditionally depends on coordination among tax authorities, financial regulators, financial intelligence units, securities authorities and sectoral agencies. In practice, these entities operate with different mandates, reporting systems, databases and priorities. When fintechs emerged as major financial intermediaries, no single authority possessed full visibility of their transactional flows, ownership structures or operational risks. Fragmentation allowed fintech activities to move between regulatory domains without generating coordinated oversight, a condition well documented in emerging markets and advanced economies alike.

The concept of non-bank financial intermediation (NBFI) further contextualizes the rise of fintech-enabled illicit finance. NBFIs—such as payment institutions, investment funds, insurance companies and asset managers—have become increasingly central to global financial systems. In

 doi:10.20944/preprints202512.0420.v1

many jurisdictions, these entities now handle a substantial share of payment flows, liquidity allocation and credit provision. However, NBFIs often fall outside prudential frameworks designed for banks. As a result, they may lack robust KYC processes, real-time monitoring, stress-testing requirements or adequate transaction-reporting mechanisms. Criminal groups exploit these weaknesses by distributing their activities across fintechs, shell companies, holding structures and informal channels.

A related concept is regulatory arbitrage, in which illicit actors deliberately select jurisdictions, institutional types or legal structures offering the weakest oversight or least stringent reporting requirements. Fintechs operating under simplified licensing regimes became attractive targets for criminals seeking to bypass bank-level scrutiny. This is evident in Brazil's recent operations, where payment institutions were used to mask the origin of funds, fragment deposits, consolidate transactions in omnibus accounts and obscure beneficial ownership. Regulatory arbitrage was amplified by disparities in reporting obligations between banks and fintechs, particularly prior to recent reforms that extended reporting requirements to payment institutions.

Finally, the framework incorporates the notion of integrated fiscal–financial crime, which recognizes that modern illicit schemes often merge tax evasion, money laundering, market manipulation, illicit trade and corporate fraud into a single operational structure. Such schemes exploit multiple systems simultaneously—tax systems, financial systems, payment networks, logistics chains and digital platforms. Fintechs provide the technological and infrastructural flexibility needed to coordinate these cross-system activities. The Brazilian cases demonstrate that illicit actors used payment institutions not simply to move funds but to integrate entire criminal supply chains, aligning financial flows with tax fraud, asset shielding and distribution networks.

Together, these concepts—parallel banking, regulatory fragmentation, NBFI vulnerabilities, regulatory arbitrage and integrated fiscal–financial crime—provide the foundation for analysing the Brazilian experience. They help explain why criminals increasingly rely on fintechs and payment institutions, and why traditional AML frameworks struggle to detect and disrupt these activities. The following section applies this framework to the major Brazilian operations, identifying how these schemes were organized, how they interacted with regulatory blind spots and how they leveraged non-bank financial channels to sustain illicit ecosystems at national scale.

3. Brazil Case Analysis: Fintechs as Parallel Banking Infrastructures

Brazil's recent large-scale investigations reveal a highly structured form of fiscal–financial crime in which fintechs and payment institutions operated as functional substitutes for traditional banks. These cases show how criminal networks exploited regulatory blind spots, technological features of digital payment systems and dispersed supervisory mandates to construct parallel banking infrastructures capable of laundering billions of reais, concealing ownership and coordinating tax evasion on a national scale.

The Carbono Oculto operation represents the clearest demonstration of this phenomenon. Investigators uncovered fintechs that processed more than R$ 50 billion in transactions through omnibus accounts that mixed payments from shell companies, fuel distributors, logistics operators, holding structures, investment funds and criminal organizations. These platforms provided anonymity and transactional opacity by allowing funds from dozens of entities to transit through a single aggregated account before being redistributed across the illicit network. Traditional bank reporting mechanisms were insufficient to capture these flows, as the underlying transactions were initiated within the fintech ecosystem rather than through bank-routed operations.

Carbono Oculto exposed a multilayered structure involving payment institutions, shell distributors, fuel formulators, transportation companies, retail service stations, fronts, holding companies and investment vehicles. Each component provided a specific operational function. Shell distributors issued invoices to simulate legitimate purchase and sale of fuel, reducing tax liabilities or avoiding them entirely. Logistics companies ensured physical movement of goods, often with documentation designed to obscure true origins. Payment institutions concentrated and redistributed

 doi:10.20944/preprints202512.0420.v1

financial flows. Holding companies and funds provided the final layer of asset shielding. The integration of these elements allowed criminal groups to operate in both the fiscal and financial domains simultaneously, merging tax evasion with sophisticated laundering practices.

The Tank operation further illustrated how fintechs facilitated parallel banking functions. Criminal groups used payment institutions to fragment cash deposits, a classic laundering technique, but adapted to the digital environment. Deposits were broken into small amounts and routed through numerous shell companies before being concentrated in fintech platforms. These entities lacked the granular monitoring obligations applied to banks and, until recent reforms, were not required to report financial movement data to the federal tax administration. The absence of these obligations enabled large-scale circulation of illicit funds without triggering traditional AML detection systems.

The Quasar operation highlighted the use of investment funds and complex corporate arrangements to obscure ownership and integrate illicit proceeds into formal markets. In this case, funds served as asset-holding structures, controlling real estate, logistics assets and other high-value properties that were shielded from enforcement actions. Transactions between related entities, some of which were supported by fintech intermediaries, created a web of financial flows designed to conceal the origins of capital. Coordination failures between securities regulators, financial intelligence units and tax authorities delayed detection and allowed these structures to grow over time.

Poço de Lobato provided another dimension to the architecture of fiscal–financial crime. The operation targeted a major fuel conglomerate whose activities included systematic nonpayment of ICMS through simulated interstate transactions, asset concealment through multi-tiered holding structures and the use of financial intermediaries to channel proceeds to controlled entities. The scale of outstanding tax liabilities, combined with the continuing economic activity of the group, revealed how criminal networks exploited fragmented enforcement among federal and state authorities. Fintech payment rails played a role in dispersing funds across jurisdictions and obscuring links between entities.

Beyond fuel distribution, the Pandora operation demonstrated that fintech-enabled laundering was also embedded in the digital commerce environment. Criminal groups created a sequence of shell companies to operate on online marketplaces, generating large volumes of sales without paying taxes. Funds received were transferred to fintech platforms, where they were mixed with other transactions and redistributed to multiple front entities. The rapid creation and dissolution of companies made it difficult for tax authorities to trace revenues, while the fintech channels provided real-time movement of capital with minimal visibility.

Taken together, these cases show that fintechs enabled not only financial anonymity but operational coordination across entire illicit supply chains. Criminal networks aligned financial flows with logistics, distribution and retail structures, using fintech platforms as the connective tissue linking these components. Each operation revealed how the convergence of digital payments, non-bank intermediation, weak reporting obligations and fragmented regulatory oversight allowed illicit ecosystems to develop scale, resilience and national reach.

These findings situate Brazil at the forefront of an emerging global trend in which fintechs serve as parallel banking infrastructures for criminal enterprises. While the magnitude of the Brazilian cases is exceptional, the mechanisms identified are not unique to Brazil. Similar risks have been documented internationally, and the lessons from these operations provide valuable guidance for developing more effective regulatory responses to fintech-enabled financial crime. The next section places these findings in comparative perspective, highlighting parallels with vulnerabilities observed in the United States, United Kingdom and European Union.

 doi:10.20944/preprints202512.0420.v1

4. International Comparison: Parallel Banking Risks in Advanced and Emerging Markets

The vulnerabilities exposed in Brazil's recent operations mirror structural weaknesses observed in several advanced and emerging jurisdictions. Although the scale and integration of criminal activity uncovered in Brazil were exceptional, the mechanisms used by illicit networks correspond to a broader global pattern in which fintechs, payment institutions and other non-bank financial intermediaries are increasingly used to circumvent traditional AML and supervisory frameworks.

In the United States, the rapid growth of payment service providers, money service businesses and digital wallet platforms created new channels for laundering and tax evasion. FinCEN has repeatedly warned that these entities enable high-volume, anonymized transactions that can bypass conventional bank monitoring. High-profile cases revealed the use of payment processors to conceal merchant identities, aggregate illicit payments and obscure financial trails. Parallel to Brazil's omnibus accounts, US investigations documented the use of pooled accounts in which illicit proceeds were mixed with legitimate transactions, making detection difficult. Regulatory oversight remains dispersed among federal and state authorities, and the absence of uniform standards for non-bank entities contributes to persistent blind spots.

In the United Kingdom, digital payment firms and electronic money institutions have been used to transfer funds across borders without adequate verification of customer identities or transaction purposes. Despite strong AML regulations, supervisory authorities identified weaknesses in onboarding procedures, beneficial ownership verification and ongoing monitoring among non-bank providers. Several enforcement actions involved platforms that served as conduits for organized crime groups moving funds between Europe, Asia and the Middle East. The UK's experience demonstrates that even jurisdictions with robust AML regimes face challenges when technological innovation outpaces regulatory adaptation.

Within the European Union, the expansion of fintechs and virtual asset service providers has created new opportunities for regulatory arbitrage across member states. Variations in licensing requirements, reporting obligations and supervisory intensity allow criminal networks to select jurisdictions with the lowest oversight burden. The EU's fragmented supervisory structure has complicated the enforcement of consistent standards, although efforts to create a unified anti-money laundering authority represent progress toward closing these gaps. VAT carousel frauds, cross-border laundering through e-money institutions and the misuse of fintechs for invoice manipulation highlight the vulnerabilities associated with non-bank intermediaries in the single market.

Emerging markets outside Latin America exhibit comparable risks. In Southeast Asia, digital wallet providers and mobile money platforms have been used to route illicit funds derived from online gambling, wildlife trafficking and tax evasion. Weak customer identification requirements and cross-border interoperability features enabled rapid movement of capital that bypassed formal banking channels. In Sub-Saharan Africa, mobile money ecosystems facilitated laundering by criminal and insurgent groups who exploited gaps in monitoring and the use of third-party agents. These cases echo the Brazilian experience: non-bank digital financial systems can be easily repurposed to support organized criminal networks when oversight mechanisms are insufficient.

Taken together, international evidence shows that fintechs and payment institutions have emerged as critical nodes in global illicit finance. Their technological flexibility, operational speed and lighter regulatory burdens make them attractive to criminal networks seeking to avoid detection or reduce compliance risk. Across jurisdictions, traditional AML frameworks designed for banks have struggled to adapt to these new channels, particularly where oversight responsibilities are fragmented among multiple authorities.

The Brazilian cases reinforce the central lesson that parallel banking infrastructures arise when regulatory frameworks do not extend equivalent monitoring, reporting and enforcement to all financial intermediaries performing bank-like functions. Similar blind spots have been observed in the United States, United Kingdom and European Union, albeit with different institutional configurations. These parallels highlight the need for international regulators to expand the

 doi:10.20944/preprints202512.0420.v1

supervisory perimeter, harmonize reporting standards and strengthen cooperation among FIUs, tax authorities and financial regulators.

The next section proposes a set of regulatory and policy measures based on the cross-country insights and the specific vulnerabilities observed in Brazil's fintech-enabled illicit finance ecosystem.

5. Policy and Regulatory Recommendations

The rise of fintech-enabled parallel banking structures presents regulators with a set of challenges that cannot be addressed through traditional banking-focused AML frameworks. The Brazilian cases demonstrate that criminal networks are capable of integrating digital payments, shell entities, tax fraud, logistics chains and investment vehicles into cohesive illicit ecosystems. To confront these risks, regulatory frameworks must evolve toward unified, cross-sector and data-rich supervisory architectures. This section proposes a set of actionable recommendations grounded in the evidence from Brazil and aligned with international best practices.

A first recommendation is the harmonization of reporting obligations for all financial intermediaries performing bank-like functions. Payment institutions, digital wallets, electronic money issuers and other fintech platforms should be subject to the same financial movement reporting standards as banks, including periodic data submissions to tax authorities, financial intelligence units and supervisory bodies. The recent extension of reporting requirements in Brazil demonstrates how quickly a regulatory correction can close a major blind spot. Extending uniform reporting obligations across non-bank intermediaries would significantly reduce opportunities for laundering and tax evasion.

A second recommendation concerns the integration of supervisory mandates. Regulatory fragmentation allows illicit networks to exploit differences between tax enforcement, AML supervision, securities oversight and sectoral regulation. Establishing permanent national coordination mechanisms that include tax authorities, the central bank, financial intelligence units, securities supervisors and sector-specific agencies would enable earlier detection of cross-cutting schemes. Shared analytics platforms, joint risk committees and real-time data exchange are essential components of an integrated approach. While ad hoc task forces have produced significant results, permanent institutional structures are needed to create continuous oversight.

A third recommendation focuses on strengthening the oversight of payment institutions and fintechs. Many of these entities rely on modular compliance arrangements, outsourced KYC functions and automated onboarding systems that may not adequately screen customers or transactions. Regulators should require enhanced due diligence for high-risk customers, impose tighter controls on omnibus accounts and mandate transparent segregation of customer funds. Monitoring the relationships between fintechs and their sponsoring banks is crucial, as the indirect access of fintechs to the financial system can obscure the true nature of transactions.

A fourth recommendation is the enhancement of beneficial ownership transparency. Investment funds, holding structures and special-purpose vehicles were instrumental in concealing assets and integrating illicit proceeds into formal markets. Regulators should require clear, up-to-date and publicly accessible beneficial ownership registries covering both domestic and foreign-controlled entities. Cross-referencing these registries with financial transaction data would improve the ability of authorities to identify suspicious multilayered corporate structures and detect asset-shielding behavior at scale.

A fifth recommendation addresses the need for cross-border regulatory cooperation. Criminal networks frequently route funds through multiple jurisdictions, taking advantage of differences in licensing standards and AML enforcement. Strengthening international information-sharing agreements, participating actively in FATF mutual evaluations and adopting interoperable reporting frameworks would help reduce opportunities for arbitrage. Engagement with global standard-setting bodies, such as the Financial Stability Board and Basel Committee, can facilitate the development of consistent approaches for supervising non-bank intermediaries across borders.

 doi:10.20944/preprints202512.0420.v1

A final recommendation concerns the alignment of fiscal and financial enforcement strategies. The Brazilian cases illustrate that tax evasion, money laundering and financial crime are deeply interconnected. Authorities must adopt an integrated enforcement framework in which fiscal crimes trigger financial investigations and vice versa. Developing joint tax–AML risk classifications for sectors such as fuel distribution, logistics, retail commerce and digital marketplaces would allow for targeted supervision. Special regulatory regimes for chronic tax evaders, combined with asset-freezing powers and coordinated civil and criminal actions, can shift the economic incentives underlying fiscal–financial crime.

Together, these recommendations provide a pathway toward strengthening the resilience of financial systems in the face of rapidly evolving illicit finance techniques. An integrated, technology-enabled and cross-sector supervisory approach is essential for preventing fintechs and payment institutions from becoming parallel banking infrastructures exploited by criminal networks. The next section concludes by summarizing the broader implications of these findings.

6. Conclusions

The evolution of fintechs and payment institutions has reshaped the architecture of financial intermediation, bringing efficiency gains but also creating new avenues for illicit activity. Evidence from Brazil's recent large-scale operations demonstrates that these entities can serve as parallel banking infrastructures when regulatory frameworks fail to extend adequate oversight to non-bank financial channels. Criminal networks leveraged these platforms to execute high-volume laundering, conceal beneficial ownership, fragment deposits, redistribute illicit capital and integrate financial flows with tax evasion and illicit trade.

The Brazilian cases illustrate how vulnerable emerging markets can be to sophisticated fiscal–financial crime when supervisory mandates are fragmented and reporting obligations are uneven across financial intermediaries. The scale and complexity of these schemes underscore the need for regulatory frameworks that recognize the systemic implications of non-bank intermediation. Traditional AML paradigms, built around the banking sector, are insufficient to address the risks posed by fintechs equipped with advanced technology, modular compliance structures and flexible transaction-routing capabilities.

The international comparison shows that similar vulnerabilities exist across advanced and emerging jurisdictions. Gaps in oversight of payment institutions, disparities in beneficial ownership rules, inconsistent enforcement of reporting obligations and limited coordination between authorities create conditions in which parallel banking systems can thrive. These vulnerabilities are not confined to any single country; they reflect structural weaknesses in global financial governance.

Addressing these risks requires a comprehensive shift toward integrated oversight. Harmonized reporting obligations, strengthened beneficial ownership transparency, enhanced supervision of fintechs, cross-sector coordination and improved analytical capabilities are essential components of an effective regulatory response. Equally important is the alignment of fiscal and financial enforcement strategies, ensuring that tax evasion and money laundering are treated as interconnected phenomena.

Fintech-enabled parallel banking represents a significant and rising threat to financial integrity, tax collection, competitive fairness and economic stability. By analysing the Brazilian experience and situating it within the broader global context, this article provides insights for policymakers, financial regulators and international organizations seeking to modernize AML frameworks and close emerging gaps. As digital financial ecosystems continue to expand, regulatory adaptation must be equally dynamic to prevent illicit actors from embedding themselves within the infrastructure of legitimate finance.

Funding: The author received no financial support for the research, authorship or publication of this article.

Data Availability Statement: No new data were created or analysed in this study. Data sharing is therefore not applicable.

 doi:10.20944/preprints202512.0420.v1

Conflicts of Interest: The author declares no conflicts of interest.

Acknowledgments: The author acknowledges the publicly available materials produced by Brazilian authorities, including reports and official communications issued by Receita Federal, Banco Central do Brasil, COAF, Procuradoria-Geral da Fazenda Nacional, state tax administrations, Ministério Público and other institutional bodies involved in national operations referenced in this study.

References

1. Agência Nacional do Petróleo, Gás Natural e Biocombustíveis – ANP (2024), *Boletim de Fiscalização do Abastecimento*, ANP, Brasília.
2. Banco Central do Brasil (2023), *Relatório de Estabilidade Financeira*, BCB, Brasília.
3. Banco Central do Brasil (2025), Resoluções BCB nº 494–498 sobre Instituições de Pagamento, BCB, Brasília.
4. Basel Committee on Banking Supervision (2021), Supervisory Practices for Managing Risks Associated with Non-bank Financial Intermediaries, BIS, Basel.
5. BIS (2023), Non-bank Financial Intermediation: Trends, Risks and Policy, Bank for International Settlements, Basel.
6. COAF – Conselho de Controle de Atividades Financeiras (2024), *Relatório de Inteligência Financeira*, Ministério da Fazenda, Brasília.
7. ESMA – European Securities and Markets Authority (2022), *Risks and Vulnerabilities in the EU Financial System*, ESMA, Paris.
8. FATF – Financial Action Task Force (2023), *Money Laundering and Terrorist Financing in the Digital Age*, FATF/OECD, Paris.
9. FATF (2021), Virtual Assets and VASPs: Updated Guidance, FATF/OECD, Paris.
10. FATF (2020), Money Laundering through the Banking Sector, FATF/OECD, Paris.
11. FinCEN – Financial Crimes Enforcement Network (2020), *Advisory on Illicit Activity Involving Convertible Virtual Currency*, U.S. Treasury, Washington, DC.
12. FinCEN (2023), FinCEN Advisory on Money Laundering Through Payment Processors, U.S. Treasury, Washington, DC.
13. Financial Stability Board (2022), Enhancing the Resilience of Non-bank Financial Intermediation, FSB, Basel.
14. Financial Stability Board (2023), Global Monitoring Report on Non-bank Financial Intermediation, FSB, Basel.
15. IMF – International Monetary Fund (2022), *The Rise of Fintech and Policy Implications for Emerging Markets*, IMF Working Paper, Washington, DC.
16. IOSCO – International Organization of Securities Commissions (2022), *Open-ended Funds Liquidity and Risk Management*, IOSCO, Madrid.
17. Juízo Federal da 3ª Região (2025), *Decisão liminar – Operação Carbono Oculto*, Justiça Federal, São Paulo.
18. Ministério da Fazenda (2025), *Nota técnica sobre lavagem de dinheiro* via *instituições de pagamento*, Secretaria Executiva, Brasília.
19. Ministério Público de São Paulo – MPSP (2025), *Relatório da Operação Carbono Oculto*, GAECO, São Paulo.
20. PGFN – Procuradoria-Geral da Fazenda Nacional (2024), *Panorama do Devedor Contumaz e Recomendações de Política Pública*, Ministério da Fazenda, Brasília.
21. PGFN/PGE-SP (2025), Relatório Conjunto sobre Operação Poço de Lobato, Governo de São Paulo.
22. Receita Federal do Brasil (2025a), Instrução Normativa RFB nº 2.278: Obrigação de Informações por Instituições de Pagamento, Brasília.
23. Receita Federal do Brasil (2025b), *Relatório Especial da Operação Carbono Oculto*, Brasília.
24. Receita Federal do Brasil (2023), *Relatório Anual de Fiscalização*, Brasília.
25. Reis, R. and Silva, L. (2023), "Payment institutions and AML blind spots in Brazil", *Revista de Administração Pública*, Vol. 57 No. 4, pp. 812–835.
26. Schindler, J. (2017), "FinTech and financial innovation: Drivers and depth", *Finance and Economics Discussion Series*, Board of Governors of the Federal Reserve System.

 doi:10.20944/preprints202512.0420.v1

27. World Bank (2022), Financial Integrity in the Digital Economy: Risks and Policy Responses, World Bank, Washington, DC.
28. Zetzsche, D., Buckley, R. and Arner, D. (2020), "The rise of digital finance and regulatory challenges", *Journal of Banking Regulation*, Vol. 21 No. 4, pp. 299–315.