Ius Gentium: Comparative Perspectives on Law and Justice 115

Doron Goldbarsht
Louis de Koker *Editors*

Financial Crime and the Law

Identifying and Mitigating Risks

Springer

Ius Gentium: Comparative Perspectives on Law and Justice

Volume 115

Ius Gentium is a book series which discusses the central questions of law and justice from a comparative perspective. The books in this series collect the contrasting and overlapping perspectives of lawyers, judges, philosophers and scholars of law from the world's many different jurisdictions for the purposes of comparison, harmonisation, and the progressive development of law and legal institutions. Each volume makes a new comparative study of an important area of law. This book series continues the work of the well-known journal of the same name and provides the basis for a better understanding of all areas of legal science.

The *Ius Gentium* series provides a valuable resource for lawyers, judges, legislators, scholars, and both graduate students and researchers in globalisation, comparative law, legal theory and legal practice. The series has a special focus on the development of international legal standards and transnational legal cooperation.

Doron Goldbarsht • Louis de Koker
Editors

Financial Crime and the Law

Identifying and Mitigating Risks

Springer

Editors

Doron Goldbarsht
Macquarie Law School
Macquarie University
Sydney, NSW, Australia

Louis de Koker
La Trobe Law School
Bundoora, VIC, Australia

ISSN 1534-6781 ISSN 2214-9902 (electronic)
Ius Gentium: Comparative Perspectives on Law and Justice
ISBN 978-3-031-59542-4 ISBN 978-3-031-59543-1 (eBook)
https://doi.org/10.1007/978-3-031-59543-1

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To our wives, Erin and Jeanne, and our
children, Arielle, Hallel, Allie and Louis.
Without their continuing support and their
sacrifices, our work would not be possible
Doron and Louis

Contents

Financial Crime and the Law: Identifying and Mitigating Risks 1
Doron Goldbarsht and Louis de Koker

The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions 15
Rhianna Hamilton and Christian Leuprecht

Financing Environmental Crime: Financial Sector Complicity in Global Deforestation and Opportunities for Regulatory Intervention . . . 43
Hannah Harris

Weeding Out Dirty Money: Cannabis Regulations and Financial Crime 71
Jamie Ferrill and Milind Tiwari

Application of the Risk-Based Approach (RBA) for Financial Crime Risk Management by Banks 101
Rachel Southworth and Michael Levi

The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges 123
Louis de Koker

Dancing in the Dark: Terrorist Financing Via the Dark Web 167
Doron Goldbarsht

Economic and Demographic Biases in FATF Mutual Evaluation Results 191
Charles Littrell

Combatting Money Laundering in Southeast Asian and Australian Casinos 225
John Langdale

FATF's Risk-Based Approach: Has the Pendulum Swung too Far? 247
Louis de Koker and Doron Goldbarsht

Contributors

Louis de Koker La Trobe Law School, Bundoora, VIC, Australia

Jamie Ferrill Australian Graduate School of Policing and Security, Charles Sturt University, Bathurst, NSW, Australia

Doron Goldbarsht Macquarie Law School, Sydney, NSW, Australia

Rhianna Hamilton Queen’s University, Kingston, ON, Canada

Hannah Harris Macquarie Law School, Sydney, NSW, Australia

John Langdale Department of Security Studies and Criminology, Macquarie University, Sydney, NSW, Australia

Christian Leuprecht Queen’s University, Kingston, ON, Canada
Royal Military College, Kingston, ON, Canada

Michael Levi School of Social Sciences, Cardiff University, Cardiff, UK

Charles Littrell Central Bank of The Bahamas, Nassau, NP, Bahamas

Rachel Southworth Australian Graduate School of Policing and Security, Charles Sturt University, Canberra, Australia

Milind Tiwari Australian Graduate School of Policing and Security, Charles Sturt University, Bathurst, NSW, Australia

Financial Crime and the Law: Identifying and Mitigating Risks

Doron Goldbarsht and Louis de Koker

Abstract In 2012 the Financial Action Task Force, the global intergovernmental standard-setter for anti-money laundering (AML), combating terrorist financing (CTF) and proliferation financing (CPF) standards embedded a mandatory risk-based approach in its standards. This has fundamentally changed AML/CTF/CPF regulatory and compliance approaches globally. This chapter considers the history behind the adoption of this approach and the implications of the approach, framing the papers in this collection.

1 Introduction

Global financial crime measures were rule-based when they originally introduced, especially in United Nations Conventions since the 1980s. Instruments such as the 1988 UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention),[1] the 1999 UN International Convention for the Suppression of the Financing of Terrorism,[2] the 2000 UN Convention against Transnational Organized Crime (the Palermo Convention)[3] and the 2003 UN Convention against Corruption[4] require countries to adopt laws to criminalise specified conduct. This approach was largely reflected of the rule-based nature of the associated criminal law.

[1] United Nations (1988).

[2] United Nations (1999).

[3] United Nations (2000).

[4] United Nations (2003).

D. Goldbarsht (✉)
Macquarie Law School, Sydney, NSW, Australia
e-mail: doron.goldbarsht@mq.edu.au

L. de Koker
La Trobe Law School, Bundoora, VIC, Australia

D. Goldbarsht, L. de Koker (eds.), *Financial Crime and the Law*, Ius Gentium: Comparative Perspectives on Law and Justice 115,
https://doi.org/10.1007/978-3-031-59543-1_1

The Financial Action Task Force, the global intergovernmental standard-setter for anti-money laundering (AML), combating terrorist financing (CTF) and proliferation financing (CPF) standards adopted a similar approach when it formulated its Forty Recommendations on combating of money laundering in 1990. Over time, that approach of the FATF shifted, in line with changes in financial supervision and financial risk management. By 2012 the FATF adopted a mandatory risk-based approach to AML/CTF and in 2020, it extended risk-based measures to its CPF standards.[5]

How did this come about? This chapter traces the history of that development and some of key motivating factors. It sets the background to the papers in this volume that explores different elements of the risk-based approach to AML/CTF/CPF.

2 Paradigmatic Transition: Rules to Risks

The FATF Recommendations, originally adopted 1990 and subsequently revised, are detailed technical standards that cover regulatory, supervisory, law enforcement, and legal issues. While the 2003 version of the revised Recommendations[6] allowed the adoption of some risk elements by regulated entities, the 2012 version embedded the risk-based approach as mandatory and core to a range of both government and institutional AML/CTF/CPF measures.

Before the introduction of risk measures, the rule-based approach held sway. In the rule-based approach the FATF standards determined the contents of domestic laws and regulations, though countries often went beyond the FATF standards[7] Domestic regulations furthermore specified the due diligence measures that regulated institutions had to employ, for example they prescribed how individuals, companies and trusts had to be identified and their identities verified.[8] Regulatory guidance often provided examples of suspicious conduct and transactions that had to be reported to financial intelligence units. The rule-based approach was not risk-insensitive. The rule-based approach generally incorporated the regulator's views of the relevant risks and appropriate mitigation of those risks.

Under the rule-based model, all participants in specific cohorts or groups were treated similarly. Rigid adherence to transparent and well-defined rules meant that the same standards were applied to all members of such groups or cohorts.

However, alongside this rigidity emerged a certain predictability, enabling malevolent actors to exploit the prescribed regulatory measures by manipulating their transactions to evade detection.

[5] See De Koker (2024), p. X.

[6] FATF (2023).

[7] De Koker (2003), p. 176.

[8] De Koker (2023).

The rule-based approach became increasingly viewed as ineffective at curbing money laundering and terrorist financing activities. For instance, in the realm of money laundering, in which perpetrators are inclined to identify and exploit regulatory gaps, the imposition of rigid rules was viewed as counterproductive. Conversely, within a dynamic regulatory landscape, the risk-based approach seemed to offer a conduit to seamlessly interlink 'detection, prevention and control' with areas that are the focal points of regulatory concern.

The formal rule-based approach also became blamed for over-compliance[9] and for over-reporting of suspicious transactions by regulated institutions. This phenomenon resulted in elevated compliance costs for private sector entities and diminished investigative capacities for financial intelligence units.[10]

Increasingly, therefore, the adoption of the risk-based measures became viewed as a corrective measure to address the bureaucratic and formalistic weaknesses of a rule-based approach. This view was not, however, informed by research and sound evidence. The process of adoption unfolded over a decade.

In 2003 the FATF standards were extensively revised. In this process optional risk-sensitive measures were introduced. For example, the key customer due diligence (CDD) standard stipulated that:[11]

> Financial institutions should apply each of the (prescribed) CDD measures..., but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

The 2003 Recommendations also set out a range of examples where simplified CDD measures may be considered[12] and countries were required to regulate and supervise financial institutions and designated non-financial businesses and professions "having regard to the risk of money laundering or terrorist financing in that sector".[13]

The introduction of the new risk elements did not lead to immediate, universal adoption. European regulators, for example, were more reluctant to dilute their rule-based approach as they were concerned about inconsistent approaches in the European Union. In 2007, under the leadership of the United Kingdom, the FATF produced its first high-level guidance of the risk-based approach.[14] This was an important opportunity for the FATF to reach internal consensus on the implications of the risk-based approach and to provide guidance on its implementation and benefits. The core benefit was summarised as follows:

[9] De Koker and Casanovas (2024).

[10] Chaikin (2009).

[11] FATF (2003) Rec 5.

[12] FATF (2003) INR5.9.

[13] FATF (2003) Rec 23, read with Rec 24.

[14] FATF (2007).

> By adopting a risk-based approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the risks identified. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, so that all financial institutions, customers, products, etc. receive equal attention, or that resources are targeted, but on the basis of factors other than the risk assessed. This can inadvertently lead to a 'tick box' approach with the focus on meeting regulatory needs rather than combating money laundering or terrorist financing.

The FATF at that stage was also aware that the benefits and challenges of the approach should be recognised. The report therefore set these out in more detail and summarised them in a box as follows[15]:

Potential Benefits:

- Better management of risks and cost-benefits.
- Financial institution focus on real and identified threats.
- Flexibility to adapt to risks that change over time.

Potential Challenges:

- Identifying appropriate information to conduct a sound risk analysis.
- Addressing short term transitional costs.
- Greater need for more expert staff capable of making sound judgments;
- Regulatory response to potential diversity of practice.

In 2010 the FATF began to consider the next significant revision of its standards. Its 2010 consultation paper consulted specifically on amendments to the risk-based elements of its standards. At that stage its concern was merely that "the current text on the Risk-Based Approach (RBA) may lack sufficient clarity, and is located in several different parts of the FATF Standards."[16] The solution it explored was to develop "a single comprehensive statement on the RBA, which could be incorporated into the FATF Standards as a new Interpretative Note dedicated to the RBA and applicable to a set of Recommendations."[17] Even though it would be in an interpretative note, the FATF was consulting on a model where with risk assessments and enhanced measures in higher risk cases would be mandatory for countries and institutions. The industry responses received from both developed and developing economies were largely supportive of the proposal, generally noting its improved resource management benefits.[18] They were similarly supportive of risk-based supervision.

The European Banking Federation, for example, supported risk-based supervision "in order to avoid supervisors and legislators applying more prescriptive rule-

[15] FATF (2007) par. 1.22.

[16] FATF (2010) par 5.

[17] FATF (2010) par 6.

[18] FATF (2011a, b).

based obligations and supervisory techniques which undermine the principles and benefits of adopting a risk-based approach to manage and mitigate money laundering and terrorist financing risks."[19]

The International Banking Federation pointed to the aftermath of the Global Financial Crises and argued that[20]:

> With the many demands placed on financial institutions around the world following recent economic turmoil, including a host of new regulations and capital requirements, emphasising the risk-based approach in AML/CTF efforts becomes increasingly important to ensure resources are targeted properly and efforts focused where they will be most productive.

In general, the message in the submissions was that financial institutions were already good at implementing the risk-based approach and welcomed a more thoughtful, broader application. The Australian Banking Association, for example, pointed out in response to the proposal on risk-based supervision[21]:

> The risk-based approach is embedded into bank AML programs and operating models. Consideration would need to be given to the impact on operations of any changes to the supervisory model.

Given this broad support expressed by industry, the FATF embedded the risk-based approach as mandatory in its 2012 standards, setting it out in Recommendation 1 and detailing it in further Recommendations and interpretative notes.

Today, the approach serves as a strategic methodology to ensure that the countermeasures implemented for the detection, evaluation, and comprehension of money laundering and terrorist financing activities align with the levels of risk identified.[22] In principle, the risk-based approach empower regulated entities to allocate resources towards sectors with heightened risk profiles that were intrinsic to their geographic location, customer demographics, and operational framework.[23] However, the information and expertise challenges that the FATF recorded in 2007 still remain. These limit the effectiveness and efficiency of the risk-based approach.[24]

3 Empowering Proactive Compliance

The contemporary landscape of AML/CTF initiatives has been fundamentally reshaped by the ascendance of the risk-based approach. Traditional regulatory responsibilities, primarily the identification of money laundering and terrorist

[19] FATF (2011b), p. 61.

[20] FATF (2011b), p. 104.

[21] FATF (2011b), p. 23.

[22] FATF (2012–2023) INR 1.

[23] De Koker (2009); Ai and Tang (2011), p. 275; FATF (2023), p. 10.

[24] De Koker and Goldbarsht (2024), p. X.

financing threats and risks and the prescription of appropriate responses, have been redistributed from traditional institutional bodies, such as regulators and supervisors to the reporting entities themselves.[25] Within this framework, reporting entities are tasked with identifying and assessing the risks that necessitate mitigation.[26] They must then devise the most fitting strategies to effectively and proportionally address the relevant risks. This recalibration reflects a shift towards a measure of AML/CTF/CPF-related self-regulation by reporting entities. The landscape now demands that these entities operate as proactive agents, playing pivotal roles in the systematic reduction of money laundering risks. This vigilance ensures the alignment of transactions with the institution's comprehensive understanding of the customer, their operational domain, and their risk propensity. Consequently, entities can no longer rely solely on established procedural norms for compliance with AML/CTF regulations.

It is important to note that the approach is not limited to financial institutions but extends to designated non-financial businesses and professions. Entities in sectors such as real estate, legal, and accounting are required to document transactions or activities earmarked as 'high risk' within those realms.[27]

The risk-based approach demands that reporting entities undertake appropriate risk assessments, tailored to their customer demographics, business frameworks, and geographic locations. This entails deploying enhanced due diligence measures where risks are assessed as higher and potentially—and optionally—simplified measures where risks are assessed as lower. However, the juxtaposition of this approach with the FATF's pre-defined and rule-based categorisation of certain customers (such as politically exposed persons) as higher risk presents a continuing paradox that further complicates the risk-based approach. Importantly, not all aspects of the FATF standards are subject to the risk-based approach. Proliferation financing for example, is for example, not fully subject to risk-based approach as simplified due diligence is not allowed in lower risk scenarios.[28]

The risk-based approach is not exact and accurate and may fail in a range of unforeseeable ways. It cannot work in a context where the regulator sets and enforces standards that in practice translates into a "zero tolerance" or an intolerant approach, i.e. where each prevention failure is viewed as a contravention of AML/CTF/CPF regulation or where negligent prevention failures attract mega fines. Within the framework, asymmetries in threat information can for example lead regulatory agencies and reporting entities to reasonably arrive at divergent views of threat levels. Regulators have to adopt a reasonable position in this regard to prevent entities from adopting overly-conservative responses[29] that limit the efficiency dividend that the risk-based approach is supposed to provide.

[25] De Koker (2009), p. 336.

[26] FATF (2012–2023), Rec 10.

[27] Goldbarsht and Benson (2023) and Bello and Harvey (2016).

[28] De Koker (2024).

[29] De Koker and Casanovas (2024).

4 Balancing Profit and Risk

The risk-based approach provides regulated entities with flexibility. Entities are responsible for categorising customers into higher and lower risk groups. The classification hinges on variables such as country or geographic risk, customer risk, and product or service risk. Exact criteria for the categories remain ambiguous, lending complexity to the task of assessing the risk levels of a customer. Customer, product and service risk assessment for each reporting entity is based on a comprehensive evaluation of the information gathered within the framework of their customer due diligence measures through the risk-based approach.[30] This process culminates in the creation of a customer risk profile.[31]

In the domain of AML/CTF, a significant challenge emerges from the fact that certain impacts, though inherently negative, can paradoxically hold financial benefit for the entity. Facilitating transactions with criminal entities seeking to launder illicit funds may yield substantial short-term gains. The act of money laundering itself does not inherently compromise the commercial interests of the facilitating organisation, whether it be a bank or a casino. The risks to the entity rather stems from other dimensions. First, such facilitation intrinsically proves detrimental to the broader society due to its potential repercussions. Second, it constitutes a proscribed activity, thereby inviting associated reputational and legal ramifications. In essence, a comprehensive evaluation of the negative impacts entails considering a range of factors, from regulatory fines to stakeholder concerns and reputational costs.

The spectrum of adverse repercussions includes the following[32]:

(i) *Regulatory sanctions*: The potential negative impact of regulatory fines hinges on the probability of detection and the magnitude of the penalty. Regulators must cultivate credibility in both elements to engender a substantiated threat. In addition to the fines themselves, organisations often incur substantial legal expenses in the immediate aftermath of regulatory intervention.

(ii) *Stakeholder impacts*: The consideration of a broader spectrum of stakeholders aligns with the recent emergence of corporate social responsibility principles. Regrettably, the diffuse repercussions of money laundering and terrorist financing often fail to resonate within organisations. Yet these adverse consequences often reverberate across national borders, affecting victims of criminal activity and terrorism in disparate countries. The more diffused the impact, the lower the likelihood that an organisation will adequately acknowledge and address it.

(iii) *Reputational risk*: Reputational risk is often a key concern but it is very difficult to assess this risk. Should an organisation's involvement in money laundering or terrorist financing become widely known that fact may impact on its stakeholder loyalty (see (ii) above, leading to customer and investor attrition

[30] Goldbarsht and de Koker (2022).

[31] Sinha (2020), p. 54.

[32] Goldbarsht and Sheedy (2024), p. X.

> and complicating recruitment and retention of staff. Costs of equity and debt capital and insurance premiums may increase and there might be a risk of loss of operational licences.[33]

AML/CTF and other risk management lapses frequently materialise due to organisational cultures that undervalue sound risk management. This in turn may result from factors such as overconfidence, a myopic short-term focus, and remuneration structures. These elements collectively hinder the cultivation of a sound risk culture within the organisation, resulting in the insufficient resourcing of risk management systems and functions, coupled with a lax approach to compliance and risk mitigation behaviour. Furthermore, red flags—indicative of potential risk scenarios—are frequently disregarded or neglected in this context. Within such an operational milieu, instances of non-compliance with risk-based methodologies become almost inescapable consequences.

The multifaceted interplay between organisational priorities, cultural attributes, and behavioural incentives underlies the landscape of AML and broader risk management failures.[34] The organisation's proclivity to emphasise goals beyond risk management is exacerbated by cognitive biases such as overconfidence, which can lead to a skewed perception of invulnerability to risks. Moreover, the prevailing culture often exalts short-term gains, leading to the prioritisation of immediate outcomes over long-term risk resilience.

The interconnectedness between cultural drivers and compensation systems should not be overlooked. Remuneration structures that disproportionately reward short-term financial success may inadvertently foster behaviour that disregards or downplays risk concerns, resulting in an imbalanced risk culture. This, in turn, engenders an environment where risk management functions are inadequately supported and risk compliance lapses do not result in appropriate penalties. Consequently, the organisation encounters a compounding deficiency in its ability to detect, address and mitigate risks effectively.

The ramifications of this compromised risk culture are manifest in a lack of resources allocated to risk management systems, leading to their inefficacy. Inadequate resourcing, coupled with a lenient stance on compliance and risk management infractions, creates a feedback loop that perpetuates a subpar risk culture. Moreover, the tendency to overlook or dismiss red flags signifies a breakdown in the organisation's ability to proactively identify and address potential risk scenarios.

Ultimately, the collective culmination of these factors results in an environment where deviations from sound risk-based approaches become almost inevitable. This manifestation of non-compliance and the accompanying ineffectual risk management strategies are a direct outcome of the organisational culture's misalignment with risk-focused imperatives. Thus, the establishment of a robust risk culture is fundamental to sound risk management within organisations.

[33] Sheedy (2021), p. 9.

[34] Sheedy (2021), p. 36.

The transition from a rule-based approach to a risk-based paradigm has also lead to important changes in the allocation of responsibilities concerning the identification of suspicious matter reports (SMRs). Much more responsibility was shifted to the wide range of reporting entities to identify what is suspicious given their risk assessments. Divergent views and concepts of 'risk' and 'suspicious" have emerged. The loss of clarity and some consistency regarding what can be viewed as suspicious has not received sufficient attention. SMRs fundamental to money laundering and terrorist financing rest on the subjective premise of 'suspicion'. In essence, an SMR serves as a notification to law enforcement regarding 'suspicious' activities of clients that might indicate potential money laundering or terrorist or proliferation financing. The decision to file an SMR is at the discretion of the reporting officer and contingent on their assessment of the risk presented by the customer or transaction.[35] The risk-based model has therefore led to a more fragmented approach to risk and suspicion, dispersing responsibility among a multitude of actors rather than centralising it within governmental purview. This has inadvertently spawned a range of interpretations of key risk-related concepts and views. Uncertainty has not led to fewer reports being filed. Risk-averse reporting entities may incline towards a conservative stance, opting for over-reporting in order to mitigate the ambiguity surrounding potentially suspect transactions.

Within this scenario, a degree of standardisation in risk discourse could be advantageous. Such standardisation could support a more consistent approach in the identification transactions to be reported. Nevertheless, caution is needed to ensure that the shift towards standardised definitions does not inadvertently lead to a reversion to rule-based regulations. The principles underlying the risk-based approach—emphasising contextual considerations and adaptive strategies—must not be diluted by an overly rigid standardisation process.

In conclusion, the migration from rule-based to risk-based paradigms has redefined the AML/CTF/CPF landscape. Wiht the benefit of experience of the risk-based approach it is opportune to evaluate its success and to consider whether modifications would be beneficial.

5 This Collection

The chapters in this collection—all of which were double peer reviewed—explore various aspects of financial crime risk management, shedding light on emerging challenges and proposing innovative solutions. Each chapter provides the author's perspective on financial crime and the measures required to combat it. Financial crime mitigation is a complex and evolving challenge in today's interconnected world. This collection thoroughly investigates various facets of the challenge, exploring innovative strategies and emerging trends across a range of critical topics.

[35] Sinha (2020), p. 56.

Through a multidisciplinary lens, it investigates the intricate interplay between financial crimes, technology, sustainability, and international cooperation.

Exploring the interplay between financial crime and cryptocurrencies reveals a complex web of connections. In their chapter (*The Crime-Crypto Nexus: Nuancing Risk across Crypto-Crime Transactions*) (Hamilton and Leuprecht 2024), Rhianna Hamilton and Christian Leuprecht critically examine the growing concern about the exploitation of cryptocurrencies for illicit activities. It analyses real-world cases of money laundering, tax evasion, and terrorism financing that utilise the anonymity and borderless nature of digital currencies. The chapter also looks into regulatory responses and the potential role of blockchain analytics in combating crypto-related financial crimes.

In response to escalating deforestation concerns, governments have enacted 'destination country laws' to criminalise the importation of illegally harvested timber. However, these regulations often overlook a significant accomplice in global deforestation: financial institutions. The chapter by Hannah Harris (*Financing Environmental Crime: Financial Sector Complicity in Global Deforestation and Opportunities for Regulatory Intervention*) (Harris 2024) investigates the unexplored territory of the financial sector's involvement in enabling harmful deforestation and facilitating illegal logging. By examining existing regulatory frameworks, it sheds light on the limitations of destination country laws. The chapter then proceeds to map how financial institutions contribute to deforestation incentives and the illicit gains from illegal logging. Ultimately, the chapter argues that conquering deforestation demands the active engagement of the financial sector, heralding a global path towards sustainable economic growth.

In their chapter (*Weeding Out Dirty Money: Cannabis Regulations and Financial Crime*) (Ferrill and Tiwari 2024) Jamie Ferrill and Milind Tiwari examine the potential relationship between cannabis regulations and money laundering. With evolving global cannabis laws and a significant market, they explore how criminal proceeds from this market might require money laundering. Amid changing regulations, the authors analyse how these changes impact the scale of money laundering. Using Australia as a case study, Ferrill and Tiwari employ the rational choice theory and empirical data to assess the influence of cannabis regulations on money laundering potential and to consider policy implications.

As discussed above, the application of a risk-based approach in managing financial crime risk is a fundamental FATF requirement, influencing legislation, regulations, and private-sector practices. In their chapter (*Application of the Risk-Based Approach (RBA) for Financial Crime Risk Management by Banks*) (Southworth and Levi 2024), Rachel Southworth and Michael Levi investigate how banks interpret and implement the risk-based approach. Challenges and variations arise in the conceptualisation and execution of the approach, impacting intelligence gathering and effectiveness measurement. Given the reliance on risk-based approach outcomes by financial intelligence units, the authors argue for a need for greater transparency in methodologies, as understanding these practical challenges is crucial to enhancing private sector participation in the financial crime control landscape.

In 2020 the FATF extended its risk-based measures to its proliferation financing standards. In his chapter (*FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges*) (De Koker 2024), Louis de Koker addresses the challenges that regulated entities face in complying with 2020 FATF amendments. Drawing on interviews with global experts and the identified challenges, the author identifies elements of appropriate national implementation strategies responding to the new standards.

As terrorists adapt to technological advancements, they employ increasingly covert financing methods. Doron Goldbarsht's chapter (*Dancing in the Dark: Terrorist Financing via the Dark Web*) (Goldbarsht 2024) dives into the underbelly of the internet—the dark web—and its role in facilitating criminal activities, including terrorism financing. It explores the challenges of monitoring and combating illicit transactions within hidden online spaces, calling for heightened technological and collaborative efforts to counteract these threats.

Addressing potential biases in national AML/CTF risk assessments, Charles Littrell's chapter (*Economic and Demographic Biases in FATF Mutual Evaluation Results*) (Littrell 2024) examines how preconceptions can impact the effectiveness of risk management strategies. This chapter empirically examines biases within the FATF's mutual evaluation reports, identifying several biases. It highlights issues such as punitive measures against economically weaker countries and biases against certain regions, including small island states and black-majority countries. The chapter highlights the need for fair and balanced jurisdictional AML/CTF assessments to ensure equity and effectiveness within the global financial ecosystem.

The centrality of casinos within the transnational crime system poses a distinct challenge in the fight against money laundering. An essential quandary surfaces as governments navigate the complex terrain of countering crime and money laundering while concurrently pursuing economic strategies aimed at bolstering employment, international tourism, and revenue generated through casinos. In his chapter (*Combating Money Laundering in Southeast Asian and Australian Casinos*) (Langdale 2024) John Langdale examines the multifaceted dynamics of money laundering within Southeast Asian and Australian casinos, contextualised within the broader framework of the East Asian transnational crime network. The chapter looks at the accelerated growth of transnational crime, particularly in regions—such as the Mekong area—with weaker governance structures. Casinos are critically examined as enablers of this criminal system, unveiling the connectivity between illicit activities and gambling establishments.

The collection concludes with a reflective chapter (*FATF's Risk-Based Approach: Has the Pendulum Swung Too Far?*) (De Koker and Goldbarsht 2024). Louis de Koker and Doron Goldbarsht reflect on some of the challenges that emerged relating to the risk-based approach and identify areas for future research.

Together, these chapters provide a comprehensive overview of the multifaceted landscape of financial crime mitigation. By thoroughly exploring each topic, the collection illuminates the complexity of the challenges at hand and emphasises the need for adaptable, multidisciplinary and collaborative approaches to effectively combat financial crimes.

References

Ai L, Tang J (2011) Risk-based approach for designing enterprise-wide AML information system solution. J Financ Crime 18(3):268–276

Bello A, Harvey J (2016) From a risk-based to an uncertainty-based approach to anti-money laundering compliance. Secur J 30(1):24–38

Chaikin D (2009) How effective are suspicious transaction reporting systems? J Money Laund Control 12(3):238–253

De Koker L (2003) Money laundering control: the south African model. J Money Laund Control 6(2):166–181

De Koker L (2009) Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance. J Financ Crime 16(4):334–352

De Koker L (2023) South Africa's initial implementation of the financial action task Force's customer identity verification standards: perspectives and reflection on regulatory processes and approaches. In: Chitimira H, Warikandwa T (eds) Financial inclusion regulatory practices in SADC. Routledge, London, 18–45

De Koker L (2024) Chapter 6: The FATF's combating of financing of proliferation standards: private sector implementation challenges. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

De Koker L, Casanovas P (2024) Chapter 3: De-risking, de-banking and denials of bank services: an over-compliance dilemma? In: De Koker L, Goldbarsht D (eds) Financial crime, law and governance, Ius Gentium: comparative perspectives on law and justice. Springer, Cham

De Koker L, Goldbarsht D (2024) Chapter 10: FATF's risk-based approach: has the pendulum swung too far? In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

FATF (2003) The forty recommendations. FATF https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202003.pdf

FATF (2007) Guidance on the risk-based approach to combatting money laundering and terrorist financing: high level principles and procedures. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/High%20Level%20Principles%20and%20Procedures.pdf.coredownload.inline.pdf

FATF (2010) The review of the standards—preparation for the 4th round of mutual evaluations. Consultation paper. https://www.fatf-gafi.org/content/dam/fatf-gafi/public-consultation/First%20public%20consultation%20document.pdf

FATF (2011a) The review of the standards—preparation for the 4th round of mutual evaluations: compilation of responses from the financial sector—Part One. https://www.fatf-gafi.org/content/dam/fatf-gafi/public-consultation/First%20public%20consultation%20document%20responses%20financial%20sector%20part%201.pdf

FATF (2011b) Consultation of proposed changes to the fatf standards: compilation of responses from the financial sector. https://www.fatf-gafi.org/content/dam/fatf-gafi/public-consultation/Second%20public%20consultation%20document%20responses%20financial%20sector.pdf

Ferrill J, Tiwari M (2024) Chapter 4: Weeding out dirty money: cannabis regulations and financial crime. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Financial Action Task Force (2012–2023) International standards on combating money laundering and the financing of terrorism & proliferation: the FATF recommendations https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html#:~:text=As%20amended%20February%202023.,of%20weapons%20of%20mass%20destruction

Goldbarsht D (2024) Chapter 7: Dancing in the dark: terrorist financing via the dark web. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Goldbarsht D, de Koker L (2022) From paper money to digital assets: financial technology and the risks of criminal abuse. In: Goldbarsht D, de Koker L (eds) Financial technology and the law. Law, governance and technology series, vol 47. Springer

Goldbarsht D, Benson K (2023) From later to sooner: exploring compliance with the global regime of anti-money laundering and counter-terrorist financing in the legal profession. J Financ Crime

Goldbarsht D, Sheedy E (2024) Money laundering and the risk in the risk-based approach: the Australian context. Monash Univ Law Rev 50(1)

Hamilton R, Leuprecht C (2024) Chapter 2: The crime-crypto nexus: nuancing risk across crypto-crime transactions. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Harris H (2024) Chapter 3: Financing environmental crime: financial sector complicity in global deforestation and opportunities for regulatory intervention. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Littrell C (2024) Chapter 8: Economic and demographic biases in FATF mutual evaluation results. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Langdale J (2024) Chapter 9: Combatting money laundering in Southeast Asian and Australian casinos. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

Sheedy E (2021) Risk governance: biases, blind spots and bonuses. Taylor & Francis Group, Abingdon

Sinha G (2020) Risk-based approach: is it the answer to effective anti-money laundering compliance? In: Benson K, King C, Walker C (eds) Assets, crimes, and the state: innovation in 21st century legal responses. Routledge, London

Southworth R, Levi M (2024) Chapter 5: Application of the risk-based approach (RBA) for financial crime risk management by banks. In: Goldbarsht D, de Koker L (eds) Financial crime and the law: identifying and mitigating risks, Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham

United Nations (1988) Convention against illicit traffic in narcotic drugs and psychotropic substances. Opened for signature 20 december 1988, 1019 UNTS 175 (entered into force 11 November 1990)

United Nations (1999) International Convention for the Suppression of the Financing of Terrorism. Adopted 9 December 1999, 2178 UNTS 197 (entered into force 10 April 2002)

United Nations (2000) Convention against Transnational Organized Crime. Adopted 15 November 2000, 2225 UNTS 209 (entered into force 29 September 2003)

United Nations (2003) Convention Against Corruption. Adopted 31 October 2003, 2349 UNTS 41 (entered into force 14 December 2005)

Doron Goldbarsht LLB, LLM (HUJI), PhD (UNSW), is the Director of the Financial Integrity Hub (FIH) and an Associate Professor at Macquarie Law School, where he teaches banking and financial crime. He is an authority on anti-money laundering and counter-terrorist financing (AML/CTF) regulations, with expertise in the related fields of compliance and financial innovation, with over 20 years of experience in the field. His recent books *Financial Crime and the Law: Identifying and Mitigating Risks* (Springer 2024, co-edited), *Financial Crime, Law and Governance: Navigating Challenges in Diverse Contexts* (Springer 2024, co-edited), *Financial Technology and the Law: Combating Financial Crime* (Springer, 2022 co-edited), and *Global Counter-Terrorist Financing and Soft Law: Multi-Layered Approaches* (Edward Elgar, 2020), as well as journal and chapter publications, focus on international AML/CTF standards and the mechanisms for their effective implementation and compliance at the national level.

Louis de Koker LLB LLM (UFS) LLM (Cantab) LLD (UFS) FSALS, is a Professor and Associate Dean: Research and Industry Engagement at the La Trobe Law School (Australia), an Extraordinary Professor at the Faculty of Law of the University of the Western Cape (South Africa) and a Board member with the Financial Integrity Hub (FIH) at Macquarie Law School. From 2014 to 2019 he was the national program leader of the Law and Policy research program of the Australian government-funded Data to Decisions Cooperative Research Centre. Louis is an expert on anti-money laundering and counterterrorist and proliferation financing, and especially the relationship between financial integrity and financial inclusion policies and regulations. Louis has worked with the Consultative Group to Assist the Poor, the World Bank, the OECD, the Asian Development Bank regulators and financial service providers on the design and implementation of appropriate integrity and inclusion over the past two decades. He has advised on a range of laws and regulations and his research on integrity laws and their impact on financial inclusion has been cited in publications of various international bodies including the World Bank, IMF, the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision.

The Crime-Crypto Nexus: Nuancing Risk Across Crypto-Crime Transactions

Rhianna Hamilton and Christian Leuprecht

Abstract Cryptocurrency is supercharging illicit activities by transnational criminal networks, including terrorism, drug trafficking, pornography, sanctions evasion, and ransomware. Yet, mainstream cryptocurrency literature often overlooks this criminal association. The relatively new and transboundary nature of cryptocurrency is restructuring criminal activities. Hacking has emerged as a digital-age bank heist, siphoning off substantial sums from exchange platforms. Crypto crime is dynamic, transitioning from primarily placing and layering the proceeds of precursor crimes into the financial system to a burgeoning trend of stealing virtual currency. While not every online financial crime involves cryptocurrency, the proliferation of crypto-enabled cybercrimes is exponential. Paradoxically, existing literature largely disregards how cryptocurrency-enabled offenses such as Online Child Sexual Exploitation and Abuse (OCSEA), sanctions evasion, and ransomware.

1 Introduction

Cryptocurrency is at the nexus of illicit behaviour by transnational criminal networks involved in terrorism, drug trafficking, pornography, sanctions-evasion, and ransomware. But you would never know it when looking at cryptocurrency literature. By way of example, a recent book on sanctions makes barely two passing

Open Access funding was made possible by the Human-Centric Cybersecurity Partnership, funded by the Social Sciences and Humanities Research Council of Canada, grant #895-2021-1007.

R. Hamilton
University of Adelaide, Adelaide, Australia

C. Leuprecht (✉)
Queen's University, Kingston, ON, Canada

Royal Military College, Kingston, ON, Canada
e-mail: christian.leuprecht@rmc.ca

D. Goldbarsht, L. de Koker (eds.), *Financial Crime and the Law*, Ius Gentium: Comparative Perspectives on Law and Justice 115,
https://doi.org/10.1007/978-3-031-59543-1_2

references to virtual currency.[1] The transboundary, un(der)regulated, and relatively new features of cryptocurrency are having a transformative impact on crime: in 2021 and 2022 a state-sponsored hacking group in North Korea procured billions in crypto coins through ransomware attacks to fund its nuclear arsenal.[2] In addition, North Korea reportedly stole $400 million in cryptocurrency in 2021 alone, which is since estimated to have grown to $1.7 billion, with crypto theft in 2022 estimated to total $3.8 billion.[3] Hacking has emerged as the crypto equivalent of a bank robbery, stealing vast sums from exchange websites: In August of 2016 Bitfinex, a top exchange program for cryptocurrency, was hacked and lost over half its digital assets. Assets valued at US$3.6 billion were traced to a couple who had enriched themselves and laundered proceeds of crime using different cryptocurrencies.[4] In other words, crypto crime is dynamic and changing; whereas virtual currencies had been primarily used to place and layer proceeds of precursor crime into the financial system, theft of actual virtual currency is a rapidly growing crime. Not every financial crime in cyberspace involves cryptocurrency; but the extent of crypto-enabled crimes in cyberspace is growing exponentially.[5] Yet, the current literature on crypto crime largely neglects the crime-crypto nexus as a subset of financial crimes related to Online Child Sexual Exploitation and Abuse (OCSEA), sanctions evasion and ransomware.

This chapter calls into question the prevalent monolithic approach to crypto crime to flag the associated inflexibility of current risk assessment frameworks for financial crime, notably as it pertains to the Financial Action Task Force (FATF), which is the dominant international organization offering guidelines on mitigating financial crimes. The chapter studies the way cryptocurrency is being leveraged to enable OCSEA, sanctions evasion and ransomware to make the case for a more nuanced approach to contain its proliferating use for criminal transactions. The sort of virtual currency in which a business deals, along with shifts in and out of one cryptocurrency or another, for instance, should affect risk scores for particularly businesses. But that is not how the system is set up. The FATF framework currently offers no flexibility for assessments and no real-time assessments. The FATF framework is allegedly over-designed for effect, rather than efficiency. What virtual currency is concerned, however, this chapter concludes that despite global Anti-Money Laundering Counter-Terrorist Financing (AMLCTF) compliance costs upwards of $270 billion a year, the current framework provides neither good traction, nor good results. That is, it is ineffective, in part because it is insufficiently nuanced to capture different types of criminogenic financial risks that emanate from the use of virtual currency. Part of the reason is inherent to the blockchain. While traditional AML is premised on precursor crime where the user is known but the

[1] Jentleson (2022).

[2] NCC Group (2023).

[3] Chainalysis (2022c, 2023b).

[4] Bilton (2022).

[5] Lin et al. (2023), p. 7.

transaction is hidden, virtual currency flips that problem: with Distributed Ledger Technology, the transaction history of the blockchain is transparent to all network nodes and non-repudiable, but the pseudonymity of individual participants is maintained, and the centralised institution replaced with the virtually currency protocol.[6]

In 2022, crypto crime netted at least $20 billion.[7] Other estimates peg profits even higher.[8] This chapter compares three types of transnational crime that stand out for their profits and particularly heinous damage: Online Child Sexual Exploitation and Abuse (OCSEA), sanctions evasion and ransomware. The use cases in this chapter show that cryptocurrency is used differently for each. OCSEA uses cryptocurrency for transactional purposes, choosing coins for pseudonymity. As technology develops to track mainstream coins used in crime, such as Bitcoin, perpetrators are shifting to more anonymous and secure methods of transaction. That partially explains a recent shift in virtual currency out of Bitcoin. For example, Monero offers greater anonymity and security. But is Monero more popular in OCSEA transactions than Bitcoin? Sanctions evasion uses cryptocurrency to transfer value and for rent seeking, when an entity aims to gain wealth without engaging in productivity or reciprocal agreements. Cryptocurrency makes it possible to move large amounts of money without a traditional transactional component. Finally, cryptocurrency is the payment of choice for ransomware attacks because amounts are large. Payments use coins such as Bitcoin but often overlap with other types of coins and mixers because proceeds subsequently need to be laundered from the initial wallet.

The subfield of crypto crime is in its infancy. Researchers are only now starting to gauge the scale of crypto crime and regulatory options to quell it. The Internet Watch Foundation, Interpol, the United Nations Office on Drugs and Crime (UNODC) have all flagged the impact, scale and proliferation of cryptocurrency-based crime on illicit economies. Still, there is little scholarship on the nexus between cryptocurrency and crime.[9] Cryptocurrency regulations remain sector-agnostic with little attention paid to illicit economies. Guidelines lack specificity and largely ignore the way crypto intersects with illicit behaviour. Cryptocurrency is changing network dynamics, geopolitical ramifications, and the dynamic of multiple criminal marketplaces. The discourse on cryptocurrency-based crime remains fairly monolithic: Should it be regulated and if so, how? What is the scale of crypto crime? Has regulation of crypto been effective?[10] Instead of taking up these basic questions, this chapter compares patterns in OCSEA, sanctions evasion and ransomware in the context of cryptocurrency. In doing so, the chapter aims to demonstrate the value of cryptocurrency as an intervening variable in these respective crimes and pivoting mitigation efforts into cryptocurrency-based crimes.

[6] Kyles (2022), p. 124.

[7] Chainalysis Team (2022a, b, c).

[8] Chainalysis (2022b), p. 23.

[9] Interpol General Secretariat (2022), UNODC (2022).

[10] Leuprecht et al. (2022), p. 324.