‘De-Risking’, De-Banking and Denials of Bank Services: An Over-Compliance Dilemma?

Louis de Koker and Pompeu Casanovas

Abstract This chapter considers the impact of drivers of over-compliance or so-called ‘gold plating’ on decisions of banks to terminate or restrict relationships with customers and counterparts. It draws on a South African study of factors that influenced overly-conservative design of anti-money laundering and counter terrorist financing measures of South African banks in a rule-based context. It considers whether the identified drivers are still relevant in a risk-based context. The chapter concludes that the broad drivers remain relevant and that regulators that wish to limit risk-informed de-banking should avoid strengthening the drivers and consider how best to neutralise them.

1 Introduction

Banks ought to comply with the law. Non-compliance holds a range of negative consequences for society, for their customers and often for the institutions themselves. Sometimes, however, banks go beyond mere compliance with the law, or act so well within the parameters of the legal requirements, that their behaviour can be called ‘over-compliant’ or may be labelled as ‘gold plating’. In theory, acting well within the law should hold benefits. Going beyond what the law requires should be

L. de Koker (✉)
La Trobe Law School, La Trobe University, Melbourne, VIC, Australia

Department of Mercantile and Labour Law, University of the Western Cape, Belville, South Africa
e-mail: l.dekoker@latrobe.edu.au

P. Casanovas
Artificial Intelligence Research Institute, Spanish National Research Council (IIIA-CSIC), Bellaterra, Barcelona, Spain

La Trobe Law School, La Trobe University, Melbourne, VIC, Australia

Institute of Law and Technology (IDT-UAB), Universitat Autònoma de Barcelona, Bellaterra, Spain

D. Goldbarsht, L. de Koker (eds.), *Financial Crime, Law and Governance*, Ius Gentium: Comparative Perspectives on Law and Justice 116,
https://doi.org/10.1007/978-3-031-59547-9_3

viewed as an expression of good corporate citizenship. This in turn should enhance trust of its regulator and its customers. It may however also hold unintended negative consequences, for example where the additional processes are more costly and divert compliance resources from higher risk areas where they are more needed. Over-compliance can limit the ability of the bank to engage in sound business opportunities and may create additional risks.[1] Calibrating compliance responses correctly to avoid non-compliance and over-compliance is, however, challenging, especially given the rise in risk-based regulation and risk-based compliance requirements in financial services.

This chapter focuses on money laundering and terrorist and proliferation financing-related bank account closures (also known as de-banking) and related denials of banking services to customers. These decisions are essentially compliance risk decisions, often driven in part by concerns that the money laundering or terrorist or proliferation financing risk and risk management costs in these cases outweigh the benefits of doing the relevant business. De-banking is often called 'de-risking', though the latter term is best reserved for cases where risk is the primary driver of the de-banking decision. De-banking decisions are causing hardship to an increasing number of customers and countries and has attracted global regulatory attention, including a closer analysis by the Financial Action Task Force, the global standard-setting body for anti-money laundering and counter terrorist and proliferation financing (AML/CTF/CPF).[2]

'De-risking' is itself a contentious label for risk-informed de-banking decisions as it labels the action solely from the perspective of the bank that limits its own risk exposure. It does so by excluding customers and transactions it views as risky. As a result, these customers and transactions are channeled into less regulated services and often the non-transparent cash economy. This in turn increases the risk of money laundering and terrorist financing harms to society, and also increases the crime risk exposure of the parties to such transactions, where these are legitimate. Ultimately, de-risking undermines global financial policies aimed at increasing access to and usage of formal financial services.[3]

De-banking is again receiving regulatory attention. Current policy initiatives range from the FATF contemplating steps to limit unintended de-risking consequences of its standards,[4] through to national agencies such as the US Treasury,[5] the European Banking Authority,[6] and AUSTRAC (Australia)[7] adopting new strategies

[1] For example, compliance with reporting and disclosure laws is importantgood but when businesses disclose more information than they are legally required to, it can affect their relationship with customers and with regulatory and supervisory bodies. Such over-compliance increases the risk of improper disclosure and data breaches. For some examples, see Klievink et al. (2018).

[2] Financial Action Task Force (2022).

[3] Global Partnership for Financial Inclusion (2016), pp. 68–69.

[4] FATF (2022).

[5] US Department of the Treasury (2023).

[6] EBA (2022); EBA (2023).

[7] AUSTRAC (2023).

and guidance to counter unnecessary de-risking, aimed at specific customer groups or more generally. In parallel, the Financial Stability Board, in collaboration with other financial standard-setting bodies and regional and national regulators are progressing with the G20 Roadmap for Enhancing Cross-border Payments, which may address concerns about de-banking impact on correspondent banking relationships.[8]

This chapter reflects on the findings of a South African study of drivers of conservative (also called "overly compliant ") AML/CTF compliance. That study helped to raise FATF's awareness of over-compliance.[9] The chapter discusses the linkages between these drivers, de-banking and the de-risking dilemma and considers technology and especially Compliance by Design and Compliance through Design measures as potential solutions. However, a brief introduction to AML/CTF/CPF is required to provide context for the discussion of conservative compliance.

2 AML/CTF/CPF Measures

Concerns about the abuse of the financial system by drug traffickers informed the decision of the G7 plus 1 meeting in Paris in 1989 to establish a task team to advise on measures to address this problem. The task team, called the Financial Action Task Force (FATF), developed a set of forty recommendations and these were adopted by the G7 in 1990 in Houston. At that meeting the task force was given the mandate to assess member countries against the measures set out in the recommendations.[10] Since 1990, this task force developed into the global standard-setter for anti-money laundering. Its mandate also broadened. In 2001, its scope was extended to counter terrorist financing. It scope broadened again in 2012 to include support for targeted financial sanctions imposed by the UN Security Council to combat proliferation of weapons of mass destruction (proliferation financing).[11]

In April 2019, after three decades of limited term mandates, the FATF was given a permanent mandate to continue its work to combat money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction. It does so primarily by setting global AML/CTF/CPF standards; encouraging their effective implementation; assessing its members for compliance and effectiveness of their AML/CTF/CPF measures; and strengthening the ability of FATF-style Regional Bodies to undertake similar assessments in relation to their members using the same assessment methodology employed by FATF.

The FATF standards require countries to adopt fairly uniform AML/CTF/CPF laws and create and maintain structures, such as national financial intelligence units.

[8] Financial Services Board (2020).

[9] See e.g. the citations in FATF (2013), n 37; FATF (2016), n 46.

[10] De Koker and Turkington (2016), pp. 244–247.

[11] De Koker (2024).

They also require countries to ensure that financial institutions and designated non-financial business and professions take prescribed measures to combat money laundering and terrorist financing. These include customer due diligence (CDD) measures. Given the focus of this chapter the discussion will be limited to the duties of banks. In terms of the FATF standards and related AML/CTF/CPF obligations, banks must undertake the following CDD measures:[12]

1. *Customer identification and verification*—determining who the customer is and, using reliable, independent source documents, data or information, verifying the customer's identity.
2. *Establishing beneficial ownership*—determining who is the actual controller of a client or beneficiary of a business relationship, service or transaction.
3. *Risk assessment and profiling*—understanding the purpose and intended nature of the business relationship. In essence the bank constructs a user profile of the customer and assesses the level of risk linked to that client and the services and products that the customer will use. In the course of this process the customer must be checked against applicable sanctions lists and blacklists. The bank must also determine whether the customer is a Politically Exposed Person (PEP). PEPs are people such as senior politicians, senior civil servants and their close relatives and close associates. They are distinguished as a group as they are viewed as potentially vulnerable to corruption.[13]
4. *Transaction monitoring and reporting*—monitoring the transactions of clients and detecting transactions that do not correlate with the transactional profile of the client. Unusual transactions that are detected must be investigated and, when there are grounds for deeming them suspicious, must be reported to the national financial intelligence unit.

Until 2012, FATF standards were predicated on a rule-based approach, requiring countries to stipulate the CDD measures banks had to implement This approach began to change in 2003 when the FATF allowed for CDD measures to be adjusted on the basis of assessed risk.[14] In 2012, however, the FATF adopted revised standards that embedded a mandatory risk-based approach to AML/CTF regulation and compliance.[15] The mandatory risk-based approach requires that national regulators and banks identify and assess their money laundering and terrorism financing risks. Where customers, services or products are assessed as posing a higher risk, enhanced CDD measures must be adopted. Where risks are lower, countries may allow their banks to adopt simplified CDD measures. Banks, in turn, may then elect to simplify their CDD for those customers, products and services posing a lower risk.

[12] FATF (2014a).

[13] FATF (2013a).

[14] FATF (2003), Rec 5.

[15] FATF (2012-2023), Rec 1. Amendments to the standards in 2020 extended a partial risk-based approach to the rule-based proliferation financing standards. For background to the 2012 developments, see Gelemerova (2009).

Proliferation financing measures were, however, excluded from the risk-based approach as they primarily support the UN Security Council's rule-based targeted financial sanctions. In 2020, however, the FATF revised its standards to require countries and regulated institutions like banks to undertake proliferation financing assessments and to adopt enhanced CDD measures where higher risks are identified.[16] Given the rule-based nature of the UN sanctions no simplification is allowed where proliferation financing risks are assessed as lower. Even low risk institutions that may benefit from a regulatory exemption from these risk assessment requirements still have to comply in full with the UN Security Council sanctions.[17]

A risk-based approach is not accompanied by regulatory provisions setting out the specific measures a regulated institution must implement to mitigate identified risks. In the AML/CTF/CPF context, for example, regulations require banks to identify and verify the identities of their customers. It is left to each bank to decide how to meet that requirement. They need to determine what would be adequate and appropriate to mitigate the relevant risks and comply with their statutory obligations to combat money laundering and terrorist financing. The FATF and some national regulators have however provided some examples of risk factors that banks can consider.[18]

The risk-based approach is viewed as an effective approach to ensure an efficient application of scarce compliance resources by focusing these resources on instances of higher risk. The approach is, however, also vulnerable to its own risks. These include the risk of failing to identify relevant risks; of assessing a risk as lower while it actually poses a higher risk; of under-designing risk control measures either by employing too few controls or not adjusting them appropriately to the level of risk, etc. This chapter focuses on the risk of overestimating risk or overdesigning risk control measures, generally referred to as "over-compliance" in the risk context.

3 Conservative and Over-Compliant Responses

Compliance generally refers to conformity with rules, i.e., following regulatory norms or demonstrating conformity with regulatory constraints.[19] As explained by Governatori, regulatory compliance is generally understood as the set of activities in

[16] FATF (2021); De Koker (2024).

[17] The FATF standards allow countries to exempt certain institutions in full or in part from AML/CFT obligations where risks are assessed as low. This exemption was extended in 2020 to the imposition of proliferation financing risk management measures on institutions, but in the latter case the impact of an exemption is limited as the institution still need to comply in full with UN Security Council sanctions. See FATF (2012-2023).

[18] See e.g. FATF (2012-2023), INR 10.

[19] The discussion in Part 2 is closely based on the report in de Koker and Symington (2014). The original article is more comprehensive and detailed, and readers are referred to it for further insights and nuances. The original figures were stylistically improved.

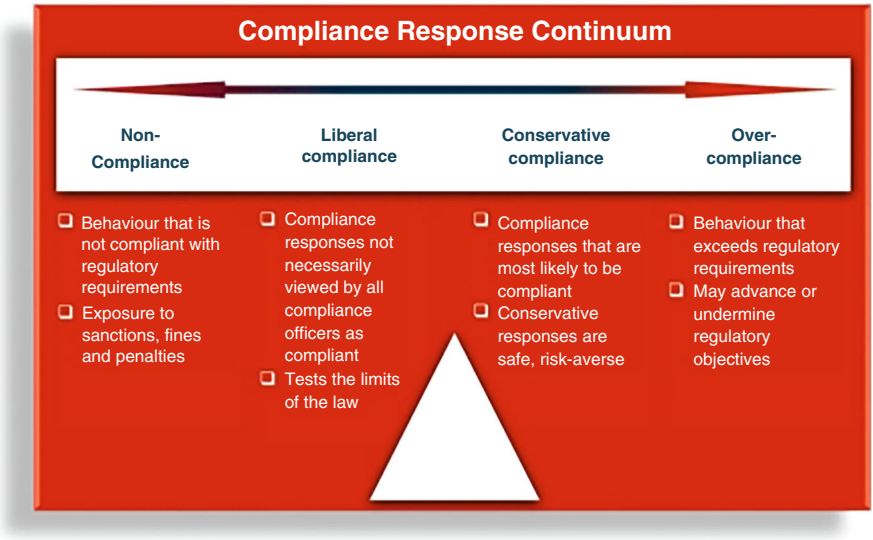

Fig. 1 Compliance Response Continuum

place in an organisation to ensure that the procedures, policies, processes and operations of the organisation comply with the normative frameworks governing the business and environment where the organisation operates.[20]

Over-compliance in a rule-based context means going well beyond what the law requires or staying very clearly well within its boundaries. See Fig. 1.[21]

The phenomenon of institutional over-compliance has been a topic of study since the 1980s, especially in relation to environmental regulations and standards.[22]

In some cases it can be adopted as a strategy, for example to signal to regulators that more stringent regulations may be adopted that would undermine competitors lacking the same capacity to comply with higher standards.[23] Wu and Wirkkala found that diverse factors may be at play, including market forces, regulatory pressure and the personal values and beliefs of senior managers regarding environmental stewardship.[24] Craswell and Calfee explored the impact of legal uncertainty on legal compliance.[25] Where penalties are large, they found that uncertain actors may wish to reduce the probability of punishment by modifying their behaviour further than the law requires.

[20] Governatori (2017), pp. 7–13.

[21] This figure was first introduced in De Koker and Symington (2014).

[22] Arora and Gangopadhyay (1995); Arora and Cason (1995); De Hart-Davis and Bozeman (2001); Gunningham et al. (2004); Gangadharan (2006); Denicoló (2008); Shimshack and Ward (2008); Wu and Wirkkala (2009).

[23] Salop and Scheffman (1983); Denicoló (2008).

[24] Wu and Wirkkala (2009), p. 401.

[25] Craswell and Calfee (1986); De Hart-Davis and Bozeman (2001), p. 476.

It has also been shown in the literature in environmental and ecological studies that 'credible enforcement significantly increases statutory over-compliance with regulations as well'.[26] However, especially in the banking sector, we should bear in mind that 'compliance is not a model of reality, but a control process exercised over the reality that unfolds'.[27]

What were, however, the factors at play in relation to over-compliance with AML/CTF obligations, especially CDD obligations? This had not been investigated before, so in 2011 a study was undertaken in South Africa to determine why banks were opting not to implement simplified due diligence measures where the law allowed them to do so. The study focused on compliance decisions that banks made in relation to a basic banking product aimed primarily at low-income individuals,[28] where regulations allowed simpler customer identity verification processes.[29]

Data for the study was collected by means of convergent interviewing of bank compliance officers using an unstructured format. The results of the semi-strucured interviews and the insights gained were discussed at two subsequent workshops with compliance and regulatory stakeholders where the findings were refined and endorsed.

In relation to the CDD measures in question the study identified 14 general drivers of conservative corporate responses by the participating institutions. These can broadly be clustered into five groups of factors, although aspects of some may resort in more than one group:[30]

1. The hard law requirement;
2. Applicable soft law;
3. Relevant business management considerations;
4. The company's own framework and reality; and
5. Supervisory conduct and relations.

4 Drivers of compliance responses

4.1 The Hard Law Requirement

Legal Uncertainty: Where the regulations were not clear, compliance officers tended to design procedures and systems that would meet the different interpretations that the regulator and the courts may give to that particular obligation, especially when the latter focus on the spirit of a law rather than the wording of a rule.[31]

[26] Shimshack and Ward (2008), pp. 90–105.

[27] Chorafas (2012), p. 103.

[28] De Koker and Symington (2014).

[29] De Koker (2006).

[30] This summary of the reasons and the text is drawn from the more detailed report in De Koker and Symington (2014). A number of clarifying improvements were made.

[31] Haines and Gurney (2003).

4.2 Applicable Soft Law

Concern about the Costs of Potential Changes: When they applied compliance measures, compliance officers tended to focus not only on current legal requirements but also on generally anticipated future requirements. Where South Africa was not yet compliant with the FATF standards, law reform to meet the standards was anticipated. This approach provided a measure of protection against costly changes to systems when the law would change. This may render them less attentive to current regulatory flexibility that they believe will or might be removed in future regulatory reforms.

4.3 Relevant Business Management Considerations

Conservative Approaches to Compliance Risk in the Industry: The interviewees indicated that the nature of their business and the need to protect their institutional reputation often informs a conservative compliance approach. As one bank compliance officer stated: "It is right and desirable that banks should be conservative."

Appropriate Management of Other Risks and Opportunities: Even though the law allowed them the option to simplify CDD there was also an understandable reluctance to simplify measures where compliance officers believed that simplified CDD may create alternative risks for the bank. Examples include when simplification may expose the bank to identity fraud, or where it may lead to a loss of business opportunities, for example limiting available customer information that is used to market alternative products to the customer.

Business Information Systems May Compel a More Conservative Approach: Where simplification required changed to the bank's business information systems banks were not able to respond immediately. Core changes to these systems are often expensive and may take years to be implemented in full. Simplified CDD required changes to customer enrolment forms and related changes to information systems and some banks were not able to implement such changes without significant expense and disruption.

4.4 The Company's Own Framework And Reality

Institutional Compliance Culture: A compliance culture can be defined as: 'The culture of shared values, beliefs, assumptions and behaviours existing within an organisation that characterises the organisation, especially in relation to compliance obligations'.[32] Compliance officers often hold that it is difficult, if not impossible, to

[32] Compliance Institute of South Africa (2007).

achieve corporate compliance in the absence of a general ethical corporate culture that supports compliance with legal obligations.[33] This culture is often called a 'sound compliance culture'.[34]

A number of interviewees identified a sound compliance culture as a reason for conservative compliance behaviour. According to these interviewees, the senior management embraced the need for, and fostered, a sound corporate compliance culture, often signalling that they wish their institutions to comply with the spirit and not merely the letter of the law. Where that was the case, compliance officers and business units would be reluctant to advise the adoption of a liberal compliance approach that may be technically correct and legal but might be viewed as challenging the spirit of the law.

Business Management Processes: In some cases business management processes informed conservative compliance responses, for example where it was easier and safer to adopt a uniformly high level of group-wide compliance to facilitate compliance management. In these cases, client enrolment procedures and requirements tended to be uniformly strict with little or no differentiation between types of individual clients.

Lack of Compliance Expertise: Compliance officers that lacked expertise or resources may over- or under-interpret the legal obligations of the institution. Given the support provided by the organised financial compliance profession in South Africa the risks of under-interpretation were low in banks but conservative over-interpretation was evident in some cases in advice to the management of the institution.

Foreign Compliance Imperatives: Banks that are subsidiaries of foreign banks or have important correspondent links with such banks often design elements of their compliance procedures to meet foreign compliance standards and requirements when those requirements exceed local requirements. This approach is supported by the standards of the FATF and the Basel Committee on Banking Supervision.[35] The study found evidence of such impact in foreign-owned banks in South Africa.

Foreign Compliance Examples: Domestic banks often looked to the processes implemented by international counterparts when they designed AML/CTF compliance responses. The legacy of older influences and the current international influences by compliance practices of counterparts, especially UK-based counterparts, inhibited a more flexible response to the South African regulations.

Management of Discretionary Requirements: Some legal requirements allowed banks to exercise discretion regarding appropriate customer enrolment processes to be followed in a given case. That discretion was normally exercised at a senior

[33] Regarding the relevance of a sound ethical corporate culture to corporate compliance, see Langevoort (2002), p. 104; Fiorelli (2004), pp. 578–580; Mintz (2005), p. 584. For the importance of an organizational culture to the success of a risk-based compliance approach see Black (2004), p. 51.

[34] Compliance Institute of South Africa (2007), Principle 12.

[35] See e.g. FATF (2012-2023), INR18.5.

management level and captured in operating procedures and rules as the view was that it would be too difficult to ensure compliance if customer contact staff were allowed to exercise their discretions. Those general rules tended to be more rigid and conservative than envisaged by the regulatory requirement.

Concern about Penalties and Sanctions: Management concern about institutional penalties as well as personal penalties and negative career consequences also impacted and informed a more cautious and conservative approach.

4.5 Supervisory Conduct and Relations

A Belief that the Regulator or Supervisor is Intolerant of Compliance Errors: When compliance officers experienced or viewed regulators or supervisors as intolerant of errors, they tend to react more conservatively.

Desire to Maintain a Good Relationship with Regulators and Supervisors: Compliance officers believed in some cases that a conservative approach preserved a good relationship with regulators and supervisors, providing access to informal guidance and enforcement leniency in case of compliance failures.

5 Modelling the Key Factors Impacting on Conservative Compliance

While much more research is required to understand the drivers and, importantly, how they interact with one another, the study prompted the design of an initial model of the impact of the five broad groups of factors identified above on each other and on the corporate compliance response decisions (see Fig. 2).[36]

A specific compliance response, as defined for purposes of the 2011 study, is primarily a response to a particular enforceable rule (the applicable *hard law* rule). CDD regulations were good examples of such binding, enforceable rules.

Soft law is also relevant. Soft law rules are rules that ar not enforceable in law but do have regulatory impact. Codes of conduct such as corporate governance codes and non-binding standards like the FATF standards are examples of soft law. For purposes of this analysis appropriate ethical principles are classified as soft law, although ethical principles can also be distinguished as a separate driver. Soft law can impact on compliance decisions by providing a lens through which the hard law rule is interpreted. Compliance officers, executive managers or courts may, for example, consider standards, codes and non-binding regulatory guidance when determining the spirit or purpose of a hard law rule. Corporate governance codes, for instance, guide banks and their directors to act ethically and to comply with their

[36]This figure was first introduced in De Koker and Symington (2014).

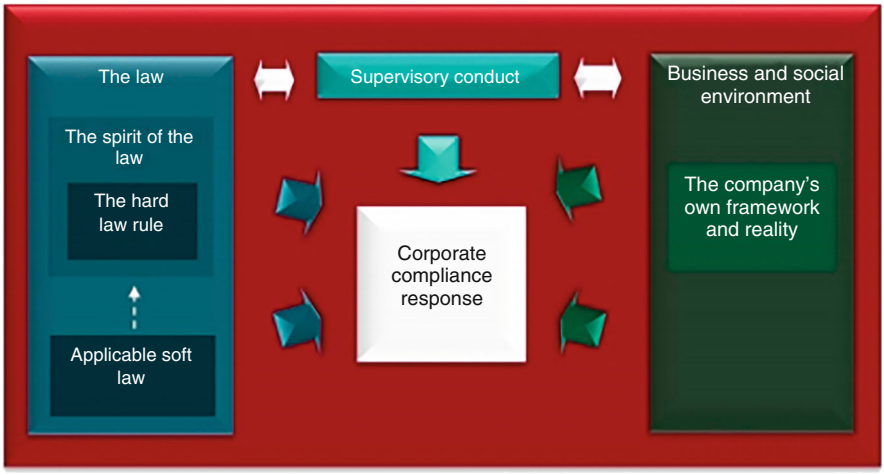

Fig. 2 Factors impacting on corporate compliance responses

legal obligations. Such principles shape corporate compliance culture and may lead companies to focus on the broader spirit, rather than the narrower language, of hard law rules.

In some cases, a soft law requirement may prompt a compliance response in its own right, even though that response is not required or enforced by the state. This may occur where the company voluntarily submits itself to compliance with that requirement, for example by signing up to an industry code.

The compliance response is also influenced by relevant *business management principles* (normal rules of commercial sustainability). These include the need to manage the business in a cost-effective manner (including managing the costs of compliance) and to manage its risks appropriately to ensure the sustainability of the business, for example protecting its reputation and continuity by avoiding crippling penalties and retaining its major business relationships and customers by maintaining trust.

The *bank's own framework and reality* includes its management's views on compliance, the company's compliance culture in general, its investment in legal and compliance capacity and resources, its financial position, etc. These factors have a significant bearing on the compliance response by the bank.

Supervisory conduct, whether actual or feared, also impacts on the compliance response. Enforcement action affects compliance by the targeted bank, but often has broader impact on compliance in the industry too. Informal signalling, such as comments in a speech by a senior supervisor, may also have impact, especially when it suggests enforcement action. Informal signalling that runs counter to action taken by the supervisor seems to have less effect, e.g., inviting banks to simplify their processes while taking harsh enforcement action when compliance failures occur.

These factors may not all be relevant or equally relevant in all cases but they do summarise and contextualise the drivers identified in the study.

6 Over-Compliance and De-Risking Denials of Services[37]

In 2014, a trend of closures of bank accounts of remittance service providers triggered global regulatory concerns.[38] An important illustration of the problem was the closure of the account of Dahabshiil, a significant cross-border remittance service provider to Somalia, by Barclays Bank in the UK. Barclays was the last large UK bank to provide services to Dahabshiil and the closure of this account threatened the continued flows of UK remittances sent by the Somalian community in the UK to family members in Somalia.[39]

The account closures of higher risk customers were not a new or unique phenomenon. It is, in fact, required by FATF standards when a financial institution finds itself unable to manage the money laundering and terrorist financing risks posed by that customer.[40] The trend of closing of accounts of small, cash-intensive businesses providing financial services to the poor was not new either.[41] However, the scale and global impact of this wave of closures caused alarm. The FATF therefore responded with a statement on 23 October 2014, expressing its concern about de-risking. It cautioned banks to implement a risk-based approach and not to engage in 'the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector'.[42] The FATF also used the statement to deny that de-risking was solely linked to AML:[43]

> De-risking can be the result of various drivers, such as concerns about profitability, prudential requirements, anxiety after the global financial crisis, and reputational risk. It is a misconception to characterise de-risking exclusively as an anti-money laundering issue.[44]

The factors listed are however closely linked to AML/CTF, especially the costs of compliance impacting on profitability; bank liquidity and financing requirements linked to risk exposure; and reputational risk that may flow from allegations that a

[37] This discussion draws on the more detailed discussion in De Koker et al. (2017).

[38] See, e.g., Migration and Remittances Team (2015); Union of Arab Banks and IMF (2015); Global Standards Proportionality Working Group (2016); Collin et al. (2015); MONEYVAL Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (2015); Durner and Shetret (2015); Scott et al. (2015); Artingstall et al. (2016); The Commonwealth (2016); Erbenová et al. (2016); Worrell et al. (2016); Alleyne et al. (2017); World Bank (2018); Woodsome et al. (2018); FATF (2022).

[39] See *Dahabshiil Transfer Services Ltd v Barclays Bank plc and Harada Ltd and another v Barclays Bank plc* [2013] EWHC 3379 (Ch); British Bankers Association (2014).

[40] FATF (2012-2023), Rec 10.

[41] Bester et al. (2008), p. 161.

[42] FATF (2014).

[43] FATF (2014).

[44] Interestingly, the 2014 statement only mentioned AML and did not specifically mention CTF or FATF's proliferation financing brief, both of which are closely linked to international political and economic sanctions. Sanctions regimes add to compliance risk concerns of banks and are often implied when the phrase AML/CTF is used.

bank allowed its systems to be abused to facilitate activities of organised crime or terror groups.

One prominent driver that has had an impact on the risk appetite of banks was the increasing size of penalties for AML/CTF-related contraventions. While million-dollar fines were imposed in serious cases in the past, the fines ballooned into the billions in 2012 when HSBC agreed to pay a then-record fine of $1.92 billion to U.S. authorities for allowing Mexican drug money to be laundered through its operations. In 2014 the record was smashed when BNP Paribas agreed to pay close on $8.9 billion in penalties because it continued to do business with countries and entities on the U.S. sanctions list.[45] Multi-million-dollar fines for AML/CTF contraventions are now standard.

Very high penalties for contravention of the AML/CTF laws combined with increased global crime, terrorism and proliferation risks globally and stricter banking standards following the global financial crisis resulted in risk averse and cost-conscious conduct by banks.[46] Higher risk customers, especially where increased compliance spending rendered the relationships unprofitable or insufficiently profitable, became primary targets of account closures.[47] Groups affected by such closures include virtual asset service providers,[48] non-profit organisations, foreign missions and diamond dealers.[49] In parallel, banks have been terminating correspondent banking relationships with other banks, where these are viewed as posing a higher risk of money laundering or financing of terrorism. These terminations have reached levels where some countries and regions of the world face a real risk of losing their access to the global financial system.[50] Despite various initial initiatives, including by the Financial Stability Board,[51] the problem still persists.

7 Conservative Compliance and the Risk-Based Approach: Perspectives on De-Risking

While the South African study was completed in an era when AML/CTF was rule-based, it is submitted that its findings are still relevant in a risk-based context.[52]

[45] See Collin et al. (2015), pp. 7–10.

[46] British Bankers Association (2014); Collin et al. (2015), p. 48; *E-Trans International Finance Ltd v Kiwibank Ltd* [2016] NZHC 1031 [149].

[47] De Koker and Turkington (2016), p. 262.

[48] De Koker and Goldbarsht (2022).

[49] Keatinge (2014), p. 16.

[50] Global Partnership for Financial Inclusion (2016), p. 70; D'Hulster et al. (2023).

[51] Financial Services Board (2019), p. 3. Financial Services Board (2020).

[52] Given that FATF's proliferation financing standards are still primarily rule-based, the relevance in relation to those standards continue.

Despite important differences in design, there are many similarities between the rule-based and the risk-based approach. Both consider and respond to money laundering and financing of terrorism risks. In the rule-based approach the regulator considers the risk and determines the risk mitigation measures in rules that the regulated community must implement. Risk assessments are not necessarily formally undertaken but sensible regulators consider risk-relevant information and data when they decide on the most appropriate risk mitigation measures that should be required. The risk-based approach shifts the risk assessment and risk management responsibility to the bank.

An important difference is of course that in a risk-based approach context, the detailed legal compliance response of a bank is a response to an identified and assessed risk rather than a response to a regulatory rule. A overly conservative response in this context could however be evident in risk identification (over-identifying risks), risk assessment (assessing lower risks as higher), and/or in risk mitigation (mitigating risks using excessive control measures).

In a risk-based context both the government and regulated institutions have risk assessment and risk mitigation responsibilities, and similar conservative responses may be evident in the national risk assessment and the design of the national regulatory framework.

A number of the key factors identified in the South African study are also evident in the circumstances that gave rise to de-risking account terminations by banks. For example:

Supervisory conduct drove a risk-averse compliance culture. The exceptionally large fines levied on HSBC in 2012 and on BNP Paribas in 2014 for CDD and other compliance failures impacted on the compliance risk appetite of the global banking industry. The FATF's 'naming and shaming' of jurisdictions that fail to comply adequately with its standards is also an important example of signalling that informs negative compliance and risk management responses in relation to the listed jurisdictions and their businesses. The responses can exceed the risk mitigation measures required.[53]

Supervisory conduct is also evident in the use of public statements by the FATF and regulators calling on banks not to engage in large-scale account closures. The positive impact of these statements was however limited as it was neutralised by ongoing enforcement actions globally resulting in huge fines for AML/CTF contraventions: Regulatory enforcement actions certainly speak louder here than senior supervisors in statements and speeches. The general lack of supervisory scrutiny of the reasons why services were denied to a specific client and of the quality of the data that informed that decision also signaled to banks that supervisors were actually not particularly concerned about the justification for denials of services.

The absence of a *hard law rule* requiring banks to manage ML/TF risk without unnecessarily exiting client relationships, for example through recognising a right to

[53] De Koker et al. (2023).

a bank account,[54] especially combined with the FATF soft law principle (supported by harder AML/CTF domestic rules) that banks should terminate relationships with clients where they believe they are not able to manage the risk relating to the relationship.

A lack of compliance expertise and resources, a factor relevant to the *company's own framework and reality*, may also play a role. Compliance officers have to be crime risk management experts to adopt sound risk-based compliance measures. They may lack that expertise and relevant data to inform risk-related decisions. Similarly foreign compliance imperatives and examples may be relevant where the bank foreign correspondent banks decide that particular relationships are higher risk or lie outside their risk appetite. Concerns about penalties and sanctions, including the impact of those on the careers of the compliance officers, may similarly inform conservative approaches to risk and risk assessment.

Compliance costs, related to the *business management principles* factor, emerged as an important factor in many bank decisions. The question is not whether the risk posed by the customer is unmanageable, but whether it could be managed profitably. Costs are often asserted but cost calculations in relation to individual relationships are rarely disclosed, if undertaken. Overdesigned controls can undermine the profitability of many business relationships.

Costs arguments are generally combined with concerns about reputational risk should abuse occur, i.e. the risk of negative impact that compliance with AML/CTF/CPF obligations may have on the bank's reputation, especially where these may be linked to a high-profile terrorism outrage. That risk is often raised but rarely quantified.[55] Reputational risk raises an important policy question: Have governments perhaps shifted too much responsibility to mitigate AML/CTF risk to the banks, with too little protection when they get it wrong? In *E-Trans International Finance Ltd v Kiwibank Ltd*[56] a bank's right to terminate a customer account as a result of ML/FT risks was challenged. The New Zealand High Court considered the interaction between the public policy aims relating to integrity in the financial markets, the important economic role of remittances for communities that relied on them, and the promotion of competition in the market.[57] Heath J remarked:[58]

> The problem is that those laudable policy aims conflict. The co-existence of statutory provisions designed to promote each of those public policy goals seems to have brought about unintended consequences. . . . By requiring private and public business enterprises to

[54] De Koker et al. (2017), pp. 151–153. This was raised as a policy option in the United States too. See Office of the Comptroller of the Currency Fair Access to Financial Services," RIN 1557-AF05 (2021). This option was however not pursued in the eventual strategy. See US Department of the Treasury (2023).

[55] Analysis, when done, often focuses on short-term movements in share markets. Ferreira (2014). Fiordelis et al. (2014) found that fraud is the event type that generates the greatest reputational damage.

[56] *E-Trans International Finance Ltd v Kiwibank Ltd* [2016] 3 NZLR 241.

[57] *E-Trans International Finance Ltd v Kiwibank Ltd* [2016] 3 NZLR 241, [142-4].

[58] *E-Trans International Finance Ltd v Kiwibank Ltd* [2016] 3 NZLR 241, [145-6].

> act as reporting entities under the Anti-Money Laundering Act, the public policy goal of minimising the risk of money laundering and financing of terrorism is promoted, but at the cost of reputational risk to financial institutions, such as Kiwibank.

Avoiding what may be viewed as significant compliance cost and reputational risk by refusing and terminating risky and unprofitable relationships is therefore a reasonable option for a compliance officer.[59] From a public policy perspective, however, that decision of the compliance officer holds significant negative consequences. For example, it undermines national crime combating objectives by compelling excluded customers to use cash and undermines economic development and financial inclusion goals by denying those customers access to formal banking services.[60]

The impact of these drivers may be amplified by the nature of the risk concepts and risk assessments that underpin the FATF's risk-based approach.

8 Objectivity of the FATF's Risk-Based Approach

The FATF does not define risk for purposes of its risk-based approach,[61] but states that 'risk can be seen as a function of three factors: threat, vulnerability and consequence'.[62]

ML/TF/PF risk assessment is not an exact empirical process following a scientific methodology that draws on sufficient evidence.[63] Much of the assessment is based on the judgments of the participants. The process is further complicated by challenges to quantify key elements of the risk concept. The FATF, for example, recognises the difficulty of assessing the consequences of ML/TF, accepting that

[59] See also Curry (2016): '[I]t it is not surprising that some banks have chosen to reduce their risks and shrink their exposure and international business portfolios. That choice is the result of what has been pejoratively labelled 'de-risking'. These withdrawals, particularly in regions subject to terrorism, drug trafficking, and other illicit activity, have been the subject of a good deal of publicity and, in some cases, have caused outcry both here and abroad. The process that has resulted in these decisions is better described as risk reevaluation. It's the process in which institutions review the risks they face on a continual basis and ensure they have systems in place that can identify and adequately address those risks. The actual process of regularly re-evaluating risk is a critical and expected part of the BSA/AML regulatory regime'.

[60] In the case of sanctions a further public policy risk was identified. When sanctions are lifted the reputation of entities and countries may not be immediately restored in the views of society and stakeholders. Banks may respond to continuing reputational risk by avoiding business with those who were previously-sanctioned, thereby undermining any sanctions relief that may have been granted. See Raynor (2022).

[61] De Koker (2011).

[62] FATF (2013b); El Khoury C (ed) (2023), pp 9–11.

[63] The FATF describes it as based on judgment: "As stated above, ideally a risk assessment involves making judgments about threats, vulnerabilities *and* consequences." See FATF (2013), pp. 7–8 and also De Koker and Goldbarsht (2024).

'incorporating consequence into risk assessments may not involve particularly sophisticated approaches',[64] and, in relation to TF risk, the FATF advised that 'countries need not take a scientific approach when considering consequences, and instead may want to start with the presumption that consequences of TF will be severe, (whether domestic or elsewhere) and consider whether there are any factors that would alter that conclusion'.[65] Conservative assumptions about consequences will tend to result in higher risk level assessments, even where the likelihood of an ML/TF/PF event is low. Furthermore, findings of serious and severe consequences are often linked to transactions regardless of the value involved (i.e. assessors adopt methodologies that assume that the consequences of a $100 MLT/TF/PF transaction and a $100,000 transaction are equally severe). This in turn elevates the chances that risk levels of smaller institutions and countries are assessed as higher than warranted.[66]

In 2022 the World Bank published a study by Ferwerda and Reuter.[67] They analysed 11 pre-2020 National Risk Assessments published by eight systemically important countries (Canada, Italy, Japan, the Netherlands, Singapore, Switzerland, the United Kingdom, and the United States) to assess their conceptual understanding and methodologies. The authors concluded:[68]

> Each raises serious issues regarding the risk assessment methodology. For example, most relied largely on expert opinion, which they solicited in ways that are inconsistent with the well-developed methodology for making use of expert opinion. They misinterpreted data from suspicious activity reports and failed to provide risk assessments relevant for policy makers. Only one described the methodology employed.

In a 2019 study Ferwerda and Kleemans raised six concerns regarding the use of expert opinions in these assessments:[69]

> Using expert opinions to assess money laundering risks has a number of disadvantages. First, virtually all experts asked to perform national risk assessments are part of the fight against money laundering. These experts might overestimate the risks of money laundering hoping to increase their AML budget in the future, or underestimate the money laundering risk for their own institutions eager to gain compliments for their 'good' fight against money laundering. Second, one might wonder whether these experts have sufficient objective information about money laundering activities—that by definition cannot be monitored—to correctly estimate money laundering risks, especially for sectors in which the expert does not work. Third, it is unclear how to aggregate expert opinions, particularly when experts differ in the undetermined amount of knowledge about money laundering risk. Fourth, even when all experts agree on a certain money laundering risk, one may wonder whether this is because this is a real risk or because they all read the same (e.g. FATF typology) reports or news articles. Fifth, using expert opinions can reinforce stereotypes instead of providing new

[64] FATF (2013).

[65] FATF (2019), pp. 8–9.

[66] IMF/World Bank (2021).

[67] Ferwerda and Reuter (2022).

[68] Ferwerda and Reuter (2022), p. 5. For earlier concerns, see Gelemerova (2009) p. 51.

[69] Ferwerda and Kleemans (2019), p. 46. Also see Southworth and Levi (2024).

and objective information. Finally, not all experts will always agree to inform the national risk assessment, which implies self-selection problems.

Institutional risk assessments, in turn, are informed by national risk assessments. The same subjectivity is present in institutional risk assessments and many of these assessments would also employ weak assessment methodologies with weaknesses similar to those that Reuter and Ferwerda identified in their study. Institutional assessments rely on the judgments of internal experts. The same questions raised by Ferwerda and Kleemans arise in relation to these assessments too. These participants may be impacted by some of the drivers outlined in 4.4 and assessments of institutional risk would then tend to be conservative. Where drivers such as these are present the design of risk mitigation measures will also be more conservative.

The over-compliance dilemma identified in the South African study may therefore be exarcerbated in the context of the risk-based approach. This may unduly impact on access to financial services[70] by denying services to customers whose risk levels are actually lower than assessed. Without constraints by rules, such as the right to access financial services,[71] or clear review standards for appropriate institutional ML/TF/PF risk assessments combined with supervisory reviews of the quality of institutional risk assessments and risk mitigation, the drivers of conservative responses can play a much larger role in these contexts.

Can new technologies assist to mitigate some of the de-risking risks?

9 Can New Compliance Technologies Assist in Countering De-Risking?

Technologies are transforming financial services. Digital financial services enable millions of customers to be serviced without associated with bricks- and mortar banking. Distributed ledger technologies like the blockchain that underpins bitcoin and crypto assets themselves may have a revolutionary impact on financial services.[72]

Technology is also impacting on traditional CDD and related compliance obligations. More countries are implementing biometric-based national identity systems that support digital identification and facilitate customer identification and verification, which in turn can lower AML/CTF compliance costs. Developments in regulatory technology (Regtech) and new collaborative CDD partnerships, often involving public-private partnerships) promise to transform compliance, increasing the efficiency and effectiveness of AML/CTF/CPF processes.[73]

[70] Bester et al. (2008); Global Partnership for Financial Inclusion (2016); FATF (2017); FATF (2022).

[71] De Koker et al. (2017), pp. 151–153.

[72] De Koker and Goldbarsht (2022).

[73] See Lyman et al. (2019), p. 1–4; De Koker et al. (2019), p. 90; Momberg and de Koker (2020), pp. 1–5.

Exciting developments are also taking place in technology-assisted compliance management, especially in relation to Compliance by Design (CbD) and AI. CbD can be defined as the relation between two sets of specifications, i.e., between the (formal) specifications of a set of regulations and the (formal) specifications of a system.[74] Thus, CbD refers to the set of formal rules that are considered in the design stage of a business or regulatory process. In the past 10 years, many formal frameworks have been proposed through a diversity of business computational languages.[75] More recently, CbD has been linked to Open Digital Rights Languages (ODRL) enabling automated business compliance checking against regulatory obligations.[76]

Can CbD assist to prevent counter the unnecessary closure of higher risk accounts? The answer unfortunately is that CbD may not provide an answer, at least not in and by itself. Clarity of the conceptual normative elements is a pre-condition of CbD, a requirement that precedes any CbD formalisation. AML/CTF is unfortunately rife with nebulous concepts. CDD is aimed at identifying suspicious transactions that may involve proceeds of crime or terrorist or proliferation financing. As has been pointed out in the literature, 'the concept of "suspicion" in itself is still vague and amorphous, proving to have a negative effect on banks to effectively identify the proceeds of crime'.[77]

To be effective in preventing over-compliance effects, the CbD formal approach should be complemented by *legal* CbD, i.e., by Compliance *through* Design (CtD). CtD aims to explicitly encompass and incorporate the social and institutional aspects that legal compliance entails—legal interpretation processes, institutionalization, the interface between modelling and coordination, and the relation between the regulated entity and citizens, consumers, and the law.[78] The more holistic CtD promises to be more useful to limit de-risking than the more formalistic CbD because it broadens and complements the CbD scope. To be successful in a risk-based approach however the CtD system needs to be informed by, and responsive to, fine-grained CDD risk data, money laundering, terrorist financing and proliferation financing data, and customer profiling data.

While risk assessment technologies are improving, much still needs to be done to improve money laundering, terrorist financing and proliferation financing risk identification and assessment systems. Much is being invested in such systems. One challenge, however, is the lack of knowledge about these activities. Our knowledge is limited to the cases of money laundering and terrorist financing that have been identified and it is generally accepted that only a small portion of these activities are correctly identified. Much of the risk may be submerged in the Rumsfeldian

[74] See Sadiq et al. (2007), pp. 149–152.

[75] Hashmi, Governatori, Lam and Wynn (2018), pp. 79–133.

[76] De Vos et al. (2019), pp. 36–51.

[77] Sinha (2014), p. 75.

[78] See Casanovas et al. (2017), pp. 33–49; Hashmi, Casanovas, and De Koker (2018), pp. 59–72; Casanovas et al. (2022), pp. 64–91.

'unknown unknowns'. Risk-based compliance systems that are designed without a broader grasp of the full risk picture, may identify mainly cases and methodologies that are similar to cases that have been identified earlier (e.g., that resemble the 'known knowns').

While CtD systems will be helpful they will, like all solutions, also breed their own problems. Coding legal rules hold its own complications[79] and coding errors may lead to expensive regulatory fines.

Given the complexity of AML/CTF/CPF, CtD applications in this context should therefore, at least at the start, have human decision makers in the loop. CtD systems may be designed to provide such humans with key information about the risks and the legal obligations to manage those risks proportionally. As appropriate data flows and the quality of CtD analysis increase, the human role may decrease.

10 Conclusion

Regulatory compliance discussions generally focus either on ensuring compliance or on the reasons for, and the impact of, failures of institutions to comply with their obligations. This chapter highlights a different problem: The risk of over-complying with the law and the negative impact of over-compliance as illustrated by the de-risking dilemma where banks have been terminating business relationships with customers and counterparts.

While technology is changing the shape of banking services it also poses intriguing possibilities of improving compliance management to prevent unnecessary de-risking. The chapter therefore also considered CbD and CtD approaches as possible solutions to the de-risking dilemma. While CbD on its own does not promise to solve the problem, CtD approaches may assist to counter de-risking-related bank account terminations and refusals. However, complex challenges await the developers of such solutions.

Regulators are clearly concerned about the levels of de-banking that is taking place. Should they wish to act more effectively to prevent ML/TF/PF risk-informed de-banking it is important to consider the drivers identified in 4.4 of this chapter. These drivers are highly relevant in the subjective, judgment-based risk assessment and risk management context of the FATF's risk-based approach.

Regulators that wish to stem de-risking should avoid strengthening any of the drivers unnecessarily, for example by making statements that would unduly inflate risk perceptions of certain types of customers or unduly inflate consequences of any criminal abuse or of minor compliance failures. Regulators should furthermore help instititions to mitigate reputational risk where, despite appropriate compliance systems, abuse occurred. Regulators can furthermore leverage the identified drivers of de-risking to address compliance-related denials of service. These drivers can be

[79] Governatori et al. (2020).

harnessed to influence the compliance decisions of banks, for example, by adopting hard law rules that recognise the rights of customers to access formal payment services. Business management and social environment factors can be leveraged by supporting collaborative CDD practices[80] that lower the costs of compliance and by providing improved risk information and data to inform institutional risk assessment and risk management of ML/TF/PF risks. Supervisory conduct can be leveraged by setting and supervising clear quality standards for institutional risk assessments and for the design and adoption of appropriate risk mitigation measures, and by reviewing the reasons way a bank denied services to a specific client or counterpart to ensure that that the reasons are sound and informed by appropriate data. A clear message that a supervisor is fair and is not trying to build a profile as the harshest policeman on the block or to create enforcement data to impress FATF mutual assessors, will also be helpful.

Acknowledgements This chapter reflects portions of text of an earlier paper on the South Africa study (De Koker and Symington (2014) in its discussion of the South African study. The chapter is based on a paper delivered at the 2018 annual conference of the German-Southeast Asian Center of Excellence for Public Policy and Good Governance (CPG), Faculty of Law, Thammasat University, in Bangkok. The authors record their appreciate to Dr. Duc Quang Ly of the CPG for his very helpful comments and editing of an earlier draft. All errors remain, however, the responsibility of the authors.

References

Alleyne T, Bouhga-Hagbe J, Dowling T, Kovtun D, Myrvoda A, Okwuokei J, Turunen J (2017) Loss of correspondent banking relationships in the Caribbean: trends, impact, and policy options. IMF, Washington DC

Arora S, Cason T (1995) Why do firms volunteer to exceed environmental regulations? Understanding participation in EPA's 33/50 program. Land Econ 72(4):413–432

Arora S, Gangopadhyay S (1995) Toward a theoretical model of voluntary over-compliance. J Econ Behav Org 28(3):289–309

Artingstall D, Dove N, Howell J, Levi M (2016) Drivers & impacts of derisking. John Howell & Co Ltd, Shamley Green

AUSTRAC (2023) Financial services for customers that financial institutions assess to be higher risk. https://www.austrac.gov.au/business/core-guidance/financial-services-customers-financial-institutions-assess-be-higher-risk

Bester H, Chamberlain D, De Koker L, Hougaard C, Short R, Smith A, Walker R (2008) Implementing FATF standards in developing countries and financial inclusion: findings and guidelines. The FIRST Initiative, Washington DC

Black J (2004) The development of risk based regulation in financial services: Canada, the UK and Australia a research report. London School of Economics and Political Science (ESRC Centre for the Analysis of Risk and Regulation), London

[80] See Lyman et al. (2019).

British Bankers Association (2014) De-risking – global impact and unintended consequences for exclusion and stability. BBA, London

Casanovas P, González-Conejero J, De Koker L (2017) Legal Compliance by Design (LCbD) and through Design (LCtD): preliminary survey. In: TERECOM-2017, Technologies for regulatory compliance proceedings of the 1st workshop on technologies for regulatory compliance, CEUR-2049, pp 33–49

Casanovas P, De Koker L, Hashmi M (2022) Law, socio-legal governance, the Internet of Things, and Industry 4.0: a middle-out/inside-out approach. J 5:64–91

Chorafas DN (2012) Basel III, The devil and global banking. Palgrave Macmillan, London

Collin M, De Koker L, Juden M, Myers J, Ramachandran V, Sharma A, Tata G (2015) Unintended consequences of anti-money laundering policies for poor countries. Centre for Global Development, Washington DC

Compliance Institute of South Africa (2007) Generally accepted compliance practice. CISA, Johannesburg

Craswell R, Calfee J (1986) Deterrence and uncertain legal standards. J Law Econ Org 2(2): 279–303

Curry TJ (2016) Remarks before the Association of Certified Anti-Money Laundering Specialists. In: 15th Annual Anti-Money Laundering and Financial Crime Conference. ACAMS, Miami. https://www.occ.gov/news-issuances/speeches/2016/pub-speech-2016-117.pdf

D'Hulster K, Morris N, Jaffer S, De Koker L (2023) The decline of correspondent banking in Pacific Island countries. Pacific Islands Forum report prepared by the World Bank https://forumsec.org/sites/default/files/2024-05/CBR%20Report_FINAL.pdf

De Hart-Davis L, Bozeman B (2001) Regulatory compliance and air quality permitting: why do firms overcomply? J Public Adm Res Theory 11(4):471–508

De Koker L (2006) Money laundering control and suppression of financing of terrorism: some thoughts on the impact of customer due diligence measures on financial exclusion. J Financ Crime 13(1):26–50

De Koker L (2011) Aligning anti-money laundering, combating of financing of terror and financial inclusion: questions to consider when FATF standards are clarified. J Financ Crime 18(4): 361–386

De Koker L (2024) 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. Springer, Cham

De Koker L, Goldbarsht D (2022) Financial technologies and financial crime: key developments and areas for future research. In: De Koker L, Goldbarsht D (eds) Financial technology and the law: combating financial crime. Springer International Publishing, Cham, pp 303–320

De Koker L, Goldbarsht D (2024) 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. Springer, Cham

De Koker L, Symington J (2014) Corporate compliance: reflections on a study of compliance responses by South African Banks. Law Context 30:228–256

De Koker L, Turkington M (2016) Transnational organised crime and the anti-money laundering regime. In: Hauck P, Peterke S (eds) International law and transnational organised crime. Oxford University Press, Oxford, pp 241–263

De Koker L, Singh S, Capal C (2017) Closure of bank accounts of remittance service providers: global challenges and community perspectives in Australia. Univ Queensl Law J 36(1):119–154

De Koker L, Morris N, Jaffer S (2019) Regulating financial services in an era of technological disruption. Law Context 36(2):90–112

De Koker L, Howell J, Morris N (2023) Economic consequences of greylisting by the Financial Action Task Force. Risks 11(5):81. https://doi.org/10.3390/risks11050081

De Vos M, Kirrane S, Padget J, Satoh K (2019) ODRL policy modelling and compliance checking. In: RuleML+RR 2019, International joint conference on rules and reasoning, proceedings, LNCS, vol 11784. Springer, pp 36–51

Denicoló V (2008) A signalling model of environmental compliance. J Econ Behav Org 68:293–303

Durner T, Shetret L (2015) Understanding bank de-risking and its effects on financial inclusion – an exploratory study. Oxfam, Oxford

EBA (2022) Opinion of the European banking authority on 'de-risking'. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf

EBA (2023) Final report guidelines on policies and controls for the effective management of money laundering and terrorist financing (ML/TF) risks when providing access to financial services. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2023/1054144/Guidelines%20on%20MLTF%20risk%20management%20and%20access%20to%20financial%20services.pdf

El Khoury C (ed) (2023) Countering the financing of terrorism: good practices to enhance effectiveness. IMF, Washington DC. https://www.elibrary.imf.org/display/book/9798400204654/9798400204654.xml

Erbenová M, Liu Y, Kyriakos-Saad N, López-Mejía A, Gasha C, Mathias E, Norat M, Fernando F, Almeida Y (2016) The withdrawal of correspondent banking relationships: a case for policy action. IMF, Washington DC

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

FATF (2012-2023) International standards on combating money laundering and the financing of terrorism & proliferation – the FATF recommendations. FATF, Paris

FATF (2013) FATF guidance: anti-money laundering and terrorist financing measures and financial inclusion. FATF, Paris. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financialinclusionandnpoissues/Revisedguidanceonamlcftandfinancialinclusion.html

FATF (2013a) FATF guidance: politically exposed persons (recommendations 12 and 22). FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf

FATF (2013b) Guidance: national money laundering and terrorist financing risk assessment. FATF, Paris. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Nationalmoneylaunderingandterroristfinancingriskassessment.html

FATF (2014) FATF clarifies risk-based approach: case-by-case, not wholesale re-risking. FATF, Paris

FATF (2014a) Guidance for a risk-based approach: the banking sector. FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf.coredownload.pdf

FATF (2016) Guidance for a risk-based approach: money or value transfer services. FATF, Paris. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-RBA-money-value-transfer-services.pdf.coredownload.pdf

FATF (2017) Guidance on AML/CFT measures and financial inclusion, with a supplement on customer due diligence. FATF, Paris. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Revisedguidanceonamlcftandfinancialinclusion.html

FATF (2019) Terrorist financing risk assessment guidance. FATF, Paris. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Terrorist-financing-risk-assessment-guidance.html

FATF (2021) Guidance on proliferation financing risk assessment and mitigation. FATF, Paris. https://www.fatf-gafi.org/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

FATF (2022) Mitigating the unintended consequences of the FATF standards. FATF, Paris. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Unintended-consequences-project.html
Ferreira S (2014) Measuring reputational risk in the South African Banking sector. North-West University, MCom. https://repository.nwu.ac.za/bitstream/handle/10394/17041/Ferreira_S.pdf?sequence=1&isAllowed=y
Ferwerda J, Kleemans ER (2019) Estimating money laundering risks: an application to business sectors in the Netherlands. Eur J Crim Policy Res 25:45–62. https://doi.org/10.1007/s10610-018-9391-4
Ferwerda J, Reuter P (2022) National assessments of money laundering risks: learning from eight advanced countries. NRAs. https://openknowledge.worldbank.org/server/api/core/bitstreams/b860c956-659e-5005-93c9-4f06993c37ab/content
Financial Services Board (2019) FSB action plan to assess and address the decline in correspondent banking: progress report 2019. FSB, Basel
Financial Services Board (2020) Enhancing cross-border payments: stage 3 roadmap. FSB, Basel. https://www.fsb.org/wp-content/uploads/P131020-1.pdf
Fiordelis F, Soana M-G, Schwizer P (2014) Reputational losses and operational risk in banking. Eur J Financ 20(2):105–124. https://doi.org/10.1080/1351847X.2012.684218
Gangadharan L (2006) Environmental compliance by firms in the manufacturing sector in Mexico. Ecol Econ 59(4):477–486
Gelemerova L (2009) On the frontline against money-laundering: the regulatory minefield. Crime Law Soc Chang 52(1):33–55
Global Partnership for Financial Inclusion (2016) Global standard-setting bodies and financial inclusion: the evolving landscape. CGAP, Washington DC
Global Standards Proportionality Working Group (2016) Stemming the tide of de-risking through innovative technologies and partnerships. Alliance for Financial Inclusion, Kuala Lumpur
Governatori G (2017) A short introduction to the regorous compliance by design methodology. In: TERECOM-2017, Technologies for regulatory compliance proceedings of the 1st workshop on technologies for regulatory compliance, CEUR-2049, pp 7–13
Governatori G, Barnes J, Zeleznikow J, Hashmi M, De Koker L, Poblet M, Casanovas P (2020) 'Rules as code' will let computers apply laws and regulations. but over-rigid interpretations would undermine our freedoms. The Conversation. 26 November 2020. https://theconversation.com/rules-as-code-will-let-computers-apply-laws-and-regulations-but-over-rigid-interpretations-would-undermine-our-freedoms-149992
Gunningham N, Kagan R, Thornton D (2004) Social license and environmental protection: why businesses go beyond compliance. Law Soc Inquiry 29(2):307–341
Haines F, Gurney D (2003) The shadows of the law: contemporary approaches to regulation and the problem of regulatory conflict. Law Policy 25(4):353–380
Hashmi M, Casanovas P, De Koker L (2018a) Legal compliance through design: preliminary results of a literature survey. In: TERECOM-2018, Technologies for regulatory compliance. proceedings of the 2nd workshop on technologies for regulatory compliance, CEUR-2309, pp 59–72
Hashmi M, Governatori G, Lam H-P, Wynn MT (2018b) Are we done with business process compliance: state of the art and challenges ahead. Knowl Inf Syst 57(1):79–133
IMF/World Bank (2021) A draft framework for money laundering/terrorist financing risk assessment of a remittance corridor. https://www.imf.org/-/media/Files/Research/imf-and-g20/2021/g20-methodology-for-remittance-corridor-risk-assessment.ashx
Keatinge T (2014) Uncharitable behaviour. Demos, London
Klievink B, Janssen M, Van der Voort H, Van Engelenburg S (2018) Regulatory compliance and over-compliant information sharing – changes in the B2G landscape. In: Parycek P, Glassey O, Janssen M, Scholl HJ, Tambouris E, Kalampokis E, Virkar S (eds) International conference on electronic government. Springer, Cham, pp 249–260
Langevoort D (2002) Monitoring: the behavorial economics of corporate compliance with law. Colum Bus Law Rev 71:71–118

Lyman T, De Koker L, Kerse M, Martin Maier C (2019) Beyond KYC utilities. CGAP, Washington, DC. https://www.cgap.org/sites/default/files/publications/2019_08_28_Working_Paper_Beyond_KYC_Utilities_0.pdf

Migration and Remittances Team (2015) Migration and remittances: recent developments and outlook special topic -financing for development, Migration and development brief, vol 24. World Bank, Washington DC

Mintz S (2005) Corporate governance in an international context: legal systems, financing patterns and cultural variables. Corp Gov 13(5):582–597

Momberg R, De Koker L (2020) Adopting SupTech for anti-money laundering: a diagnostic toolkit. Bankable Frontiers Associates: Regtech for Regulators Accelerator. https://bfaglobal.com/wp-content/uploads/2020/06/R2A-AML-SupTech-Toolkit-04June2020-1.pdf

MONEYVAL Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (2015) 'De-risking' within MONEYVAL states and territories. Council of Europe, Strasbourg

Office of the Comptroller of the Currency (2021) Fair access to financial services RIN 1557-AF05. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-8a.pdf

Fiorelli P (2004) Will U.S. sentencing commission amendments encourage a new ethical culture within organizations? Wake Forest Law Rev 39:565–586

Raynor B (2022) The shadow of sanctions: reputational risk, financial reintegration, and the political economy of sanctions relief. Eur J Int Rel 28(3):696–721. https://doi.org/10.1177/13540661221100540

Sadiq S, Governatori G, Naimiri K (2007) Modeling of control objectives for business process compliance. In: Alonso G, Dadam P, Rosemann M (eds) Business process management. Springer, Heidelberg, pp 149–164

Salop S, Scheffman D (1983) Raising rivals' costs. Am Econ Rev 73(3):267–271

Scott P, Schryer-Roy A-M, Murphy B, Pomfret E (2015) Hanging by a thread: the ongoing threat to Somalia's remittance lifeline. Oxfam, Oxford

Shimshack J, Ward M (2008) Enforcement and over-compliance. J Environ Econ Manag 55(1): 90–105

Sinha G (2014) To suspect or not to suspect: analysing the pressure on banks to be 'policemen'. J Bank Regul 15:75–86

Southworth R, Levi M (2024) 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. Ius Gentium: comparative perspectives on law and justice, vol 115. Springer, Cham. https://doi.org/10.1007/978-3-031-59543-1_5

The Commonwealth (2016) Disconnecting from global finance de-risking: the impact of AML/CFT regulations in commonwealth developing countries. Commonwealth Secretariat, London

Union of Arab Banks, IMF (2015) The impact of de-risking on MENA banks. IMF, Washington

US Department of the Treasury (2023) The department of the treasury's de-risking strategy. https://home.treasury.gov/system/files/136/Treasury_AMLA_23_508.pdf

Woodsome J, Ramachandran V, Lowery C, Myers J (2018) Policy responses to de-risking: progress report on the CGD Working Group's 2015 recommendations. Centre for Global Development, Washington DC

World Bank (2018) The decline in access to correspondent banking services in emerging markets: trends, impacts, and solutions lessons learned from eight country case studies. The World Bank, Washington DC

Worrell D, Brei M, Cato L, Dixon S, Kellmann B, Walrond S (2016) De-risking in the Caribbean: the unintended consequences of international financial reform. Central Bank of Barbados, Bridgetown

Wu JJ, Wirkkala T (2009) Firms motivations for environmental over-compliance. Rev Law Econ 5(1):399–433

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 of 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.

Pompeu Casanovas [h-Index: 37] is a Research Professor at the Research Institute on Artificial Intelligence of the Spanish Research Council (IIIA-CSIC), and an Adjunct Professor at La Trobe Law School and the Autonomous University of Barcelona. He has been a Key Researcher of the Australian government-funded Data to Decisions Cooperative Research Centre (2017–2019) and Research Professor at the La Trobe Law School (2017–2021). He is also Director of Advanced Research, and he has been founder and Head, of the Institute of Law and Technology at the Autonomous University of Barcelona (IDT-UAB) (2005–2020). At present, he is leading the IDT SGR 00534 (funded Research Group of Excellence, Catalan Government, 2022–2025). He has been Key or Principal Researcher in over 100 national, European, and international projects, and has authored, co-authored or edited about 30 books (in three different languages) and more than 150 scientific articles on AI, cybersecurity, regulatory models, the semantic web, and intellectual history.