

Supporting the Combating of Financing of Weapons of Mass Destruction with AI Technologies*

Louis de Koker^{1,2}

¹La Trobe LawTech, La Trobe Law School, La Trobe University, Melbourne, VIC 3086, Australia

²Department of Commercial and Labour Law, University of the Western Cape, Bellville, Cape Town 7535, South Africa

Abstract

The anti-money laundering and combating the financing of terrorism compliance obligations are becoming increasingly complex for large banks. To meet these obligations, these banks are increasingly relying on regulatory compliance technologies, also known as "regtech". The use of AI technologies enhances the ability of regtech to perform complex tasks such as rating customer risk and identifying potential suspicious transactions. With the adoption of new risk assessment and risk mitigation standards for proliferation financing (PF) of weapons of mass destruction, there is a greater need for appropriate and improved regtech. This paper provides an overview of the development of these standards, their relationship with AML/CFT standards, and the common areas where regtech can be applied to meet AML/CFT obligations. It also highlights some of the legal risks associated with relying on regtech in this space. Regulators, compliance officers, and technologists must navigate these risks to ensure that appropriately-designed regtech can be used to increase global financial integrity and security.

Keywords

Regtech, proliferation financing, FATF, anti-money laundering

1. Introduction

Large banks are increasingly relying on compliance technologies, known as "regtech" to meet their anti-money laundering (AML) and combating of financing of terrorism (CFT) regulatory obligations [1]. Where AI technologies are employed regtech's usefulness to undertake more complex task such as rating the risk of customers and identifying potential suspicious transactions is enhanced. The need for appropriate and improved regtech increased with the adoption of new risk assessment and risk mitigation standards in relation to proliferation financing (PF) of weapons of mass destruction.

This brief paper provides a short overview of the development of the latter standards, their relationship with AML/CFT standards and some of common areas of application of regtech to meet AML/CFT obligations. It concludes by highlighting a few cases that illustrate some of the remaining legal risks related to reliance on regtech in this space. These risks will need to be navigated by regulators, compliance officers and technologists to ensure that the power


Proceedings of Artificial Intelligence Governance Ethics and Law (AIGEL), Reviewed, Selected Papers. November 02 - December 19, 2022, Barcelona, Spain

✉ L.DeKoker@latrobe.edu.au (L. d. Koker)

ORCID 0000-0003-0120-6150 (L. d. Koker)



© 2022 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

of appropriately-designed regtech can be harnessed to increase global financial integrity and security.

The paper reflects initial perspectives gained in a study of the implementation of FATF's PF standards, especially their 2020 extension to require countries and AML/CFT/CPF-regulated institutions (such as banks) to undertake PF risk assessments in relation to targeted financial sanctions of the United Nations Security Council and to adopt enhanced control measures where risks are found to be higher. Interviews were conducted with key FATF, FATF-style regional bodies, proliferation and PF experts, compliance consultants, development experts, as well as compliance officers representing global, large and smaller banks.

2. Background

In January 2022 the Science and Security Board of the Bulletin of the Atomic Scientists placed the hands of the Doomsday Clock at 100 second to midnight, the same placement position it held since 2020. On 24 January 2023 the clock hand was moved 10 second later to 90 seconds to midnight. This is the closest to midnight - the nightmare hour of global catastrophe - in its 75-year existence. The increasing nuclear risk linked to the war in Ukraine, the continuing investment of the Democratic Republic of North Korea in its nuclear program, and the fragility of international non-proliferation agreements added to this assessment [2].

Given this risk, proliferation measures – broadly defined as measures aimed at combating the acquisition and use weapons of mass destruction (WMD) – should enjoy priority attention globally. While there is a broad measure of consensus that chemical and biological weapons should not be produced and used, politics, however, complicate discussion and action on nuclear proliferation and these complications are evident in a lack of consensus and weak agreements on action where agreement is reached [3].

Against this backdrop, the Financial Action Task Force (FATF), the global intergovernmental standard-setting body for anti-money laundering (AML) and combating of financing of terrorism (CFT), was given the mandate to also combat proliferation financing (PF), i.e. financial or economic support for proliferation [4]. FATF standards have a powerful impact as they determine contents of national regulations and of compliance programs of regulated financial institutions (e.g. banks, insurance companies, etc.) and designated businesses and professions (lawyers, accountants, real estate agents, etc.) worldwide. Countries that fail to FATF standards effectively may suffer negative economic impact linked to their non-compliance [5]. Banks and other regulated institutions that fail to comply with AML/CFT laws face penalties that may run into billions of dollars [6].

The FATF mandate was however restricted to support for targeted financial sanctions (TFS) adopted by the United Nations Security Council (UNSC) under Chapter VII of the United Nations Charter against countries whose proliferation activities are deemed to threaten peace or constituted breaches of the peace or acts of aggression [7]. In practice, that means that the FATF measures are focused on support for UNSC sanctions against Iran and North Korea. It is furthermore restricted to the UNSC's TFS in relation to those two countries, i.e. those sanctions levied on named entities and individuals, and do not extend to general activities that are listed as part of the UNSC's activity-based sanctions [8].

Despite the relative ease with which these PF-TFS measures could be implemented through name-scanning against the sanctions lists, implementation was slow. A FATF report in 2022 on the levels of compliance and effectiveness of the implementation of their standards found that levels of effectiveness with this set of PF-TFS obligations to be largely unsatisfactory, with 52% of FATF members and 82% of FATF-style regional body members rated either low or moderate. Only 34% of the 59 sampled jurisdictions transposed UNSC designations without delay. In more than two-thirds of countries, financial institutions demonstrated on average a medium-to-high understanding of their obligations regarding PF-TFS but designated non-financial businesses and professions had a poor to unclear understanding in 70% of cases [9].

FATF's presidency rotates and the improvement of the FATF's contribution to combating proliferation financing standards was a goal of the 2018-2019 US presidency of FATF [10]. This resulted in 2020 in the adoption of enhanced standards that required countries and their AML/CFT/CPF-regulated institutions to undertake PF-TFS risk assessments and to adopt enhanced control measures where higher risks were identified [7, 11].

The new risk assessment and risk mitigation requirements are not trivial. They require access to information and the capacity of each regulated institution, large or small, to correctly assess how their products and services may be used to evade targeted UNSC financial sanctions.

FATF's PF-TFS measures can make a meaningful contribution to non-proliferation if implemented effectively and efficiently. This brief paper identifies some of the implementational challenges regarding PF-TFS and useful contributions that AI technologies can make to increase the effectiveness and efficiency of the relevant measures.

3. AML/CFT

In 1989 the G7 created a task force to advise on how best the large economies can protect their financial systems against drug-related money laundering abuse. In 1990 the task force, known as the Financial Action Task Force (FATF), produced 40 recommendations [8] [12]. These recommendations have since developed into global standards. Each country is assessed by the FATF framework for their level of technical compliance with the standards and, since 2013, also for the effectiveness of their measures. Countries that are deemed to fall short, may be grey- or blacklisted. Risk management requirements that apply to listed countries hold negative economic impacts and listed countries generally work hard to reach the required compliance levels to be delisted [5].

The FATF standards create a framework where financial institutions and designated non-financial businesses and professions must identify and verify the official identities of their customers. They must also profile their customers and use these profiles to identify unusual and suspicious transactions that may involve proceeds of crime. Collectively these measures comprise "customer due diligence" (CDD) measures [8]. Should concerns remain after internal investigations these transactions must be reported to national financial intelligence units that must support law enforcement agencies with appropriate financial intelligence. Certain standard transactions, for example large cash transactions, may also be made reportable by countries whether or not they are suspicious.

In 1996 the FATF framework was extended to proceeds of all serious offence and in 2001 to

financing of terrorism using legitimate funds or proceeds of crime [12]. In 2012 the FATF's scope was extended to support UNSC targeted sanctions in relation to proliferation financing, as discussed in 2. FATF-related control measures have also become aligned with and embedded in institutional compliance with national and global economic sanctions regimes.

In practice, FATF measures require AML/CFT/CPF-regulated institutions to collect, manage and analyze a large body of data. Customers have to be identified by collecting specified identity particulars, e.g. name, date of birth, national identity number (if any), residential address, etc. This data must be verified in a manner specified by the institution's risk-based compliance framework, e.g. comparing the name to a government-issued document with the person's official name and photograph or other reliable, independent data or information [13].

Information must also be collected to understand how the customer wishes to use the services and to profile the customer to anticipate transaction patterns [8]. The patterns that can be expected of a student's account would differ from that of a salaried civil servant or a small entrepreneur and deviations from expected behaviour would trigger a closer investigation by the regulated institution.

In addition, the FATF, in an effort to combat corruption, require regulated institutions to determine whether any of their customers are foreign Politically Exposed Person or PEPs, and to obtain senior management approval to provide services to such customers. PEPs, especially foreign PEPs, are deemed to be at higher risk of PEPs are viewed as more vulnerable to bribery and corruption. They include senior politicians, senior military and judicial officers and senior government officials, their family members, close associates, and senior executives of any state-owned business enterprise are defined as PEPs [8]. PEP status can frequently change, e.g. after a national election. Identifying whether a customer is a PEP or not, whether in your country or elsewhere, requires PEP data and continuous customer scanning and data collection [14].

These tasks become even more complicated when the client is a company or a trust as the regulated institutions must attempt to identify the natural persons who are the beneficial owners and controllers of the client.

Since 2012 the FATF embraced a mandatory risk-based approach, requiring countries and institutions to undertake money laundering and terrorist financing risk assessments and adopt enhanced AML/CFT control measures where higher risks are identified. Where lower risks are present, countries may allow their institutions to simplify their CDD measures [8]. The risk-based approach requires ongoing risk assessment processes. These in turn require analysis of appropriate data to determine changes in risk levels and the design and implementation of appropriate risk mitigation measures.

Regulated institutions therefore have to maintain different processes for customers depending on their risk profiles and these profiles change as the customer's own activities and relationship change over time. For large institutions that is a formidable task that can only be performed when supported by appropriate technology.

4. AML/CFT, data and data technologies

Over the course of the past two decades large regulated financial and other institutions invested significant amounts in appropriate information systems to manage their customer due diligence obligations [15].

New standards gave rise to obligations to access new data. When the PEP measures were introduced, for example, there was a need to access data to identify PEPs in the existing customer data base and to verify statements by new customers that they are not PEPs [14]. Countries refused to compile national lists of PEPs and therefore banks turned to the market. Vendors like WorldCheck, since acquired by Refinitiv, was established to collect public data on PEPs, sanctioned individuals and entities and other customers that may be of interest to regulated financial service providers for example arms dealers and persons publicly linked to organised crime. While such data was useful it still required human capacity to consider the information and inform appropriate decisions by senior management whether to commence, continue or terminate a relationship with a controversial or higher risk customer.

The need for increased human compliance expertise increased institutional compliance costs. In 2022 LexisNexis estimated the total cost of financial crime compliance across financial institutions worldwide to be 274.1 billion, up from 213.9 billion in 2020 [16]. After FATF's adoption of the mandatory risk-based standards in 2012, it led to "de-risking" or risk-related de-banking of higher risk customers and sectors. De-risking is described by the FATF as the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach. De-risking affects a range of customers and sectors such as money remittance providers, correspondent banks, charitable organisations, PEPs, fintech and workers in the legitimate sex industry [17]. Despite expressions of concern by policymakers that de-risking may impede the access of small countries to the global financial system, and numerous statements criticizing de-risking, policy action to address it still remains limited.

At an industry level there has been developments to save compliance costs by outsourcing some of the customer identification and verification functions to a provider or an industry body generally called a "Know-Your-Customer (KYC) utility". These can operate in various forms as a collaborative CDD vehicle [18]. These have proved challenging to set up and operate profitably, especially given the data protection and commercial confidentiality challenges that they need to navigate, but these collaborative CDD relationships and networks continue to hold great promise to increase the effectiveness of CDD measures while limiting costs [19].

With the increased digitalization of financial service and the rising trend of fintech innovation attention began to turn to regtech – technologies that embed or facilitate regulatory compliance – and suptech – technologies that support supervisory bodies to oversee compliance by regulated institutions [1]. Global bodies and national regulators began to organise techsprints to support the development of technologies that could support more effective and efficient – also cost-efficient – AML/CFT/CFR compliance [20].

In the same period, technology also began to pose increasing risks to AML/CFR/CPF policy objectives. Blockchain technology enabled the development of virtual assets and pseudonymous transactions that could evade AML/CFT/CPF control measures. New business models were adopted that fell outside the existing regulatory scope. Criminal abuse of these products

increased. In June 2019 FATF therefore adopted standards requiring the registration or licensing of virtual asset service providers (VASPs) [21, 22]. New technologies also increased cyber security and data protection risks that could undermine AML/CFT/CPF control measures.

The FATF in July 2021 published a report on opportunities and challenges of new technologies for AML/CFT. While security, data protection and human-technology interaction were identified as major challenges, important opportunities were identified for AI technologies were recognized [23]:

The increased use of digital solutions for AML/CFT based on Artificial Intelligence (AI) and its different subsets (machine learning, natural language processing) can potentially help to better identify risks and respond to, communicate, and monitor suspicious activity. At public sector level, improved live (real-time) monitoring and information exchange with counterparts enable more informed oversight of regulated entities, helping to improve supervision. At private sector level, technology can improve risk assessments, onboarding practices, relationships with competent authorities, auditability, accountability and overall good governance whilst cost saving.

The report, for example, identified a few examples of the potential value to be added by machine learning. These include [32]:

- Identification and verification of customers: Where institutions deal with remote customers AI, including biometrics, machine learning and liveness detection techniques, can be used to perform micro expression analysis, anti-spoofing checks, fake image detection, and human face attributes analysis.
- Monitoring of the business relationship and behavioural and transactional analysis: Unsupervised machine learning algorithms can use behaviour to group customers and enable tailored and efficient monitoring of the business relationship.
- Identification and implementation of regulatory updates: Machine Learning techniques combined with Natural language processing, cognitive computing capability, and robotic process automation can scan unstructured regulatory data sources on an ongoing basis inform compliance decisions and processes.

5. PF-TFS and technology

The non-proliferation sanctions discussed earlier are being evaded by a range of actors. North Korea is an example of a state that is building a nuclear program in defiance of international agreements to prevent the spread of these technologies. Non-state parties such as terrorist groups are also seeking access to these technologies. Non-proliferation control measures are evaded by professional proliferators. A network operated by AQ Kahn, a Pakistani scientist who enabled the development of Pakistan's uranium enrichment capabilities, for example, assisted other countries such as Iran, Libya and North Korea with their programs [24]. Many of the methods used were and are similar to those used by money launderers and terrorist financiers to evade detection and law enforcement. Proliferators for example commit fraud and use front

companies and obscure beneficial ownership to order controlled goods. Good may ostensibly be ordered for use in a third country but diverted en route or re-directed to a country of concern [25].

Analysing transactions that may involve proliferation activities to identify potential PF-TFS-relevant activities is challenging. Proliferation often involve so-called controlled goods (such as arms) and especially dual-use goods, i.e. technology that can be abused to construct WMD or applied for civilian purpose such as medical applications. These goods are normally identified and described in lists issued by government. Where banks provide trade finance bank compliance officers are required to identify when goods subject to export controls may be involved in a specific transaction without the required permission having been obtained. Lack of sufficient technical knowledge to identify the relevant goods, especially when they are not described using the language in the list of controlled goods, will undermine the effectiveness of a bank's compliance processes. Proliferators also evade controlled goods processes by exporting goods that fall below the specifications of listed controlled goods but can be upgraded for WMD use when received at the final destination. Many bank compliance officers do not necessarily have the technical expertise to identify relevant trade transaction.

Bank compliance officers need to understand which countries pose a higher proliferation risk. Often controlled goods are not exported directly to these countries but diverted to other countries from where they will be shipped to their final destination [7, 25]. Some countries are more likely to be such transit destinations, often linked to their geographical position and also their political relationship with the country of final destination.

In addition to supporting human decision-taking by filling gaps in expertise, AI technologies may fulfil a range of other helpful functions too. Schörnig investigated the use of AI as an WMD arms control tool and points to a range of additional helpful functions that AI technologies may perform such as translation of technical texts from languages such as Russian, Farsi, Korean, Arabic and Swahili; interpretation of fast-changing rules and embedding them in Compliance by/through Design into compliance processes [44]; analysis of visual data, e.g. images of freight haulage and storage; integration of multi-modal data (the above and more, e.g. communications, media and social media, etc); and data visualisation to support human decision-taking, where required [26].

That said, the standards, though ambitious in some respects, are minimum standards. Countries and their regulated institutions are therefore able to go beyond these standards and related laws when they design their FATF-related compliance measures Banks, for example, may extend their proliferation financing measures beyond UNSC targeted financial sanctions. While such an extension will support broader non-proliferation, it will also be more challenging than PF-TFS. Appropriate technology, especially when available to the regulated industry as a whole, will greatly lessen implementational challenges.

Developers of AI technologies to support proliferation financing will need to navigate a few barriers. Schörnig, for example, points out that in the proliferation context “the events AI has to be trained for are very rare but have very serious consequences” [26]. In addition to analysing big data on customers, AI also have to be trained on thin datasets of examples of evasion of proliferation controls. The fact that we have a relatively small number of PF evasion examples will impact the quality of AI tool. That impact, however, will not necessarily undermine their effectiveness compared to human detection, given the limited available of appropriate human

expertise. Compliance professionals across the regulated industries globally have to be informed and trained on new examples and, given the scale of human involvement in AML/CFT/CPF, this would inevitably alert the proliferators to the known typologies. Inevitably they would simply adopt alternative approaches to evade human detection. AI technologies may therefore not be at a significant disadvantage compared to human detection capabilities in this space.

6. Legal regtech hurdles to navigate

While technologists grapple with the design of regtech that would provide appropriate support for AML/CFT/CPF compliance, compliance officers are grappling with regulatory liability regarding the use of regtech. In general, regtech is viewed as a merely a tool and it does not shift the ultimately institutional responsibility for non-compliance from the regulator to the designer. The compliance function of the institution must however be comfortable with the technology, understand its strengths and limits; and be able to compensate for the latter. They are the “human(s) in the loop” of AI regtech in this space [27], but their involvement may not be particularly beneficial unless they are appropriately skilled and resourced. Two recent Australian cases involving two of Australia’s largest banks show that it should not be assumed that the relevant humans have the required skills and resources.

In June 2018, AUSTRAC, the Australian AML/CFT/CPF regulator, agreed to a AUD 700 million (EUR 435 million) penalty with the Commonwealth Bank of Australia (CBA) to resolve Federal Court proceedings relating to serious breaches of AML/CTF/CPF laws [28]. Key charges related to the failure of CBA to introduce appropriate controls to mitigate and manage the ML/TF risks of new Intelligent Deposit Machines (IDMs) smart ATMs, that were able to accept deposits. CBA failed to provide 53,506 threshold transaction reports (TTRs) to AUSTRAC on time from November 2012 to September 2015, having a total value of about *A625million.ATTRisareportthatshouldbe filedforeachcashtransactionsof A10,000 or more.*

The 53,506 TTRs relate to cash deposits via the IDMs. When IDMs were introduced CBA designed and implemented an automated process to identify threshold transactions and to report them to AUSTRAC. The process identified transactions by transaction codes. Two transaction codes were used to identify the types of deposits involving cash that could be made through IDMs, being transaction codes 5022 and 4013. In June 2012, an issue was identified regarding an error message. To address that error message, a third transaction code was introduced for certain cash deposits through IDMs, being transaction code 5000. At that time, however, the TTR process was inadvertently not updated and configured to respond to transactions with the transaction code 5000 with a view to filing an AUSTRAC report. This was clearly the result of human error. As a result, cash deposits through IDMs identified by transaction code 5000 did not automatically generate TTRs from 5 November 2012 to 1 September 2015 [29].

In 2020, Westpac, another large Australian bank agreed a AUD 1,3 billion (EUR 806 billion) fine with AUSTRAC [30]. Its serious breaches of AML/CFT/CPF laws included the failure to report to AUSTRAC all International Funds Transfer Instructions (IFTIs) that it received or sent. The bank failed to report approximately 19.5 million IFTIs over a 6-year period. Non-compliance was due to technology failings and human error. Most of the failings could be traced back to the design and implementation program of the IFTI program in 2009, where the bank stated [31]:

... resource constraints in the relevant technology team impacted the successful implementation of the project. In 2011/12, there was also a high turnover of staff where a whole team departed to join another organisation. The loss of continuity and specialist knowledge associated with these departures contributed to the implementation errors.

These experiences – and the fines – are sobering. They do have a chilling impact on the appetite to employ technology where there is concern about the institutional compliance capacity to identify and correctly manage the attendant technology and technology implementation risks.

In addition, institutions also need to be mindful of attitudes of the regulators. Regulators tend to be conservative, especially in the AML/CFT/CPF space, and may not support the use of technology for certain compliance functions.

The use of machine learning and AI technologies to support AML/CFT compliance featured recently in a compliance dispute in the Netherlands. The Dutch central bank, De Nederlandsche Bank (DNB) took action for non-compliance against the digital challenger bank, Bunq, who was using data analytics to perform some of its compliance functions [32]. On appeal, the some of the conclusions reached by DNB was upheld but the most important conclusions were overruled.

As pointed out above in 3, a key compliance obligation of a bank is to understand the purpose and intended nature of the business relationship when an account is opened. That understanding informs the risk profile and expected transaction profile of the customer. This in turn is then used to identify outlier transactions for further investigation and potential reporting to the authorities as suspicious.

While new business customers were asked questions about their activities and intended use of the new account, Bunq had a large number of existing customers that were not asked those questions. Bunq used its data about those customers, including data about their behaviour, to construct their profiles. (par 8.5.2). The data included the user identity, expected monthly transaction volume, formal business activity description (according to the Chamber of Commerce), and company activities. (par 8.5.4) The DNB rejected that approach as insufficient as it believed that Bunq had to collect that profiling information from each customer. While such profiles are generally constructed before account opening, the DNB conceded that they can be adjusted during the relationship based on new information or transactional patterns that may form. (par 8.5.4) Given that the relevant legislation does not prescribe how the customer due diligence should be performed, the appellate board found that the DNB has not proved that Bunq failed to establish the purpose and intended nature of the individual business relationships. It therefore ruled in Bunq's favour.

Bunq's approach to the intended use and transaction profile of private (i.e. non-business) customers was somewhat different. (par 8.6.1). Bunq distinguishes between two segments of private customers (peer groups): (i) a group of customers who fall within the 'regular user' profile and who use the current account within the limits of 'regular use', and (ii) a group of customers who do not fall within the 'regular user' profile and/or who do not use the Bunq payment account within the 'regular use' limits.

Bunq compiled the following regular user profile based on an analysis of data from its customers and the use of the current account by customers:

Age of customers:	8-60 years
Country of residence:	Netherlands, Belgium, Germany, Austria, Italy, Spain or France
Purpose:	Standard Payment Account (Monthly outgoing)
transaction volume:	EUR 10,000
Maximum balance:	EUR 10,000
Number of payments per month:	Up to 150

According to Bunq's analysis of its current customers the vast majority of its private customers fall within this profile and use Bunq's payment account accordingly.

Based on this analysis, new customers are initially assigned this profile. Bunq then uses the data collected during the account registration process, as well as information that Bunq subsequently collects about the customer (such as transaction behaviour), to check whether a customer remains within the regular user profile. When this is no longer the case, Bunq - depending on the risk profile of the relevant customer and the customer's deviations from the regular user profile - automatically asks the customer a number of questions. The customer's file is also manually reviewed. If a customer does not answer these questions within the set period, the customer will be (temporarily) denied access to the account. Using the new information the customer's profile is updated and the customer is no longer classified as a regular user.

In addition, Bunq treats non-regular users differently. Bunq's data analysis shows that, statistically, non-regular users form a higher risk. As a consequence, the risk profile of these customer is adjusted upwards. Customers with a higher risk profile are subject to more intensive transaction monitoring.

DNB rejected this approach of assigning the same 'regular user profile' to every client falling within the general group (par 8.6.2.) It argued that, by failing to obtain specific information from the client in advance, Bunq has insufficient insight in advance into the nature and purpose of the relationship and therefore into the possible risks that the service entails. The standard profile is based on assumptions rather than collected facts.

The appeal board found in this respect in favour of Bunq. The board held that DNB failed to show why the information obtained by Bunq via data analysis and statistical research was insufficient to determine the purpose and intended purpose for private customers who want to open a payment account and who fall within the 'regular user profile'. It held that DNB did not contradict Bunq's argument that, statistically speaking, a vast majority of its private customers fall within this profile and use the current account in a similar way. Bunq has furthermore established on the basis of statistical analysis that the risk of fraud among these customers is smaller than customers who do not fall within that profile (par 8.6.4.) The appellate board therefore found in Bunq's favour on this aspect too.

DNB also argued that Bunq's continuous monitoring of its customers was defective because it was applying the statistically-generated risk profile rather than a specific risk profile informed by data obtained from each individual customer. DNB argued that Bunq only asked questions after deviations have been detected from the pre-filled standard values. Given the earlier finding that DNB did not prove that these profiling processes of Bunq were defective, this argument about monitoring was also rejected.

Bunq's processes regarding PEP checks and the quality of its investigation into the source of

the funds of customers were however held to be non-compliant.

Bunq's appeal was largely successful and its use of data analytics and statistics was supported by the appeal board. DNB's conservative approach to the use of data analytics and machine learning is however somewhat sobering. DNB has been very progressive in relation to technology but even progressive regulators and supervisors may need a nudge to adjust their approaches and allow financial institutions to embrace advanced data technologies to support their compliance functions. Until they signal clearly to the market where reliance on technology would meet statutory compliance requirements and the conditions that would apply for such reliance to enjoy the support of the regulator, the industry may not fully embrace the benefits of the relevant technology.

7. Conclusion

AML/CFT measures aim to minimize the risk of organized crime and terrorism globally. These are important objectives but arguably not as important as the objectives of non-proliferation. Here the risks are dire. The task of preventing the financing of weapons of mass destruction outside the norms of international law and the frameworks of international agreements is, however, complex. If regulated institutions such as banks are to perform this task well they will need appropriate regtech. Designing that technology will be a complex task that will require governments, technologists, proliferation scientists, trade experts, criminologists and compliance professionals to collaborate. In addition a regulatory framework will need to be created that will enable institutions and their compliance officers to rely on such technology without undue exposure to legal risk. The cases mentioned in this paper reflect some of the complexity that regulators will need to consider when these technologies are used and overseen by imperfect institutions, teams and individuals. Careful thought should also be given to access to the technology. Smaller institutions may be at risk of abuse if they are unable to afford the expensive regtech that large banks can employ. Gaps in the financial industry can undermine the effectiveness of PF measures. Collaboration, especially collaborative CDD, will therefore be ideal.

Acknowledgments

The support of SOAS; Wolfson College, Oxford; the Faculty of Law of the Autonomous University of Barcelona, and especially the IDT-UAB; the IIA-CSIC and all the kind colleagues of these institutions are gratefully acknowledged.

References

- [1] L. De Koker, N. Morris, and S. Jaffer, "Regulating Financial Services in an Era of Technological Disruption", *Law in Context* 36.2 (2019): 90-112.
- [2] Science and Security Board, "2023 Doomsday Clock Statement".
- [3] A. Debs and N. P. Monteiro, *Nuclear Politics*, Cambridge, Cambridge University Press, 2017.

- [4] Financial Action Task Force, "Declaration of the Ministers and Representatives of the Financial Action Task Force", 2012.
- [5] L. De Koker, "Economic Impact of FATF Greylisting", Proc. Third Bahamas Empirical Anti-Money Laundering Conference, Central Bank of the Bahamas, Nassau, 20-21 January 2022 (2022).
- [6] M. Collin, L. De Koker, M. Juden, J. L. Myers, V. Ramachandran, A. Sharma, and G. M. Tata, "Unintended consequences of anti money laundering policies for poor countries", Centre for Global Development (2015).
- [7] Financial Action Task Force, "Guidance on Proliferation Financing Risk Assessment and Mitigation" (2021).
- [8] Financial Action Task Force, "International Standards on Combating Money Laundering and The Financing Of Terrorism & Proliferation: The FATF Recommendations" (2012-2022).
- [9] Financial Action Task Force, "Report on the State of Effectiveness and Compliance with the FATF Standards" (2022).
- [10] Financial Action Task Force, "Objectives for the FATF during the US Presidency 2018-2019" (2018-2019).
- [11] <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf>, accessed June 2021.
- [12] L. De Koker, and M. Turkington, "Transnational organised crime and the anti-money laundering regime", *International law and transnational organised crime*, 2016: 241-263.
- [13] Financial Action Task Force, "Guidance on Digital Identity" (2020).
- [14] L. De Koker, "Applying anti-money laundering laws to fight corruption", in: A. Graycar, *Handbook of global research and practice in corruption*, Cheltenham, Edward Elgar, 2011, pp. 340-358.
- [15] Hong Kong Monetary Authority, "AML/CFT Regtech: Case Studies and Insights" (2021).
- [16] <https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report>
- [17] L. De Koker, S. Singh, and J. Capal, "Closure of Bank Accounts of Remittance Service Providers: Global Challenges and Community Perspectives in Australia", *University of Queensland Law Journal* 36 (2017).
- [18] T. Lyman, L. De Koker, C. Martin Meier, and M. Kerse, "Beyond KYC Utilities: Collaborative Customer Due Diligence" (2019), <https://www.cgap.org/blog/series/beyond-kyc-utilities>
- [19] F. Diepenmaat, "(The Fight Against) Money Laundering: It's All About Networks", in: O. M. Granados and J. R. Nicolás-Carlock (Eds.), *Corruption Networks: Concepts and Applications 2021*, Springer, Cham, pp. 115-130.
- [20] https://www.bis.org/hub/g20_techsprint.htm
- [21] <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>, accessed October 2021.
- [22] L. De Koker, T. Ocal, and P. Casanovas, "Where's Wally? FATF, Virtual Asset Service Providers, and the Regulatory Jurisdictional Challenge", in D. Goldbarsht, and L. De Koker, (Eds.), *Financial Technology and the Law : Combating Financial Crime*, Springer International Publishing, Cham, 2022, pp. 151-183.

- [23] Financial Action Task Force, "Opportunities and Challenges of New Technologies for AML/CFT" (2021).
- [24] P. F. Ikonou, *Global Nuclear Developments: Insights from a Former IAEA Nuclear Inspector*, Springer, Cham, 2020, pp. 25-66.
- [25] J. Brewer, "Study of Typologies of Financing of WMD Proliferation - Final Report", Centre for Science and Securities Studies, King's College, London, (2017).
- [26] N. Schörnig, "Artificial Intelligence as an Arms Control Tool: Opportunities and Challenges", in: T. Reinhold, and N. Schörnig (Eds.), *Armament, Arms Control and Artificial Intelligence: The Janus-faced Nature of Machine Learning in the Military Realm*, Springer, Cham, 2022, pp. 57-72.
- [27] D. A. Zetsche, D. W. Arner, R.P. Buckley, and B. Tang, "Artificial Intelligence in Finance: Putting the Human in the Loop", *Sydney Law Review* 43 (2020).
- [28] AUSTRAC: 'AUSTRAC and CBA agree \$700m penalty' (2018).
- [29] <https://www.commbank.com.au/guidance/newsroom/CBA-and-AUSTRAC-resolve-AMLCTF-proceedings-201806.html>, accessed Federal Court of Australia, NSD1305 of 2017.
- [30] N. Locke, and H. Bird, "Perspectives on the current and imagined role of artificial intelligence and technology in corporate governance practice and regulation", *Perspectives on the Current and Imagined Role of Artificial Intelligence and Technology in Corporate Governance Practice and Regulation* (February 9, 2020). *Australian Journal of Corporate Law*, 2020.
- [31] Westpac Group: 'Westpac Releases Findings into AUSTRAC Statement of Claims Issues' (2020).
- [32] *Bunq BV v De Nederlandsche Bank (DNB)* (2022).