3

Know Your Red Flags: Detecting Trends and Patterns in Financial Crime

Moran Harari, Dimitrios Kafteranis, Markus Meinzer, Lucas Millan-Narotzky, and Alison Schultz

3.1 INTRODUCTION

In response to high-profile money laundering scandals, global and EU anti-money laundering (AML) frameworks have been significantly strengthened (Ates et al. 2025a; Jackson et al. 2023). Obliged entities (OEs) such as banks, real estate agents, and lawyers are now required to file suspicious transaction reports (STRs) under broadened criteria, and growing awareness – especially after record fines imposed on major financial institutions – has led to a sharp increase in filings (Cusack 2022). As a result, Financial Intelligence Units (FIUs) and law enforcement agencies (LEAs) face a mounting volume of STRs, often with limited resources to process them (FATF-GAFI 2022 p. 37; Lando & Landry 2023 p. 3). Given the high proportion of false positives, effective systems for red flagging by OEs and for STR analysis and prioritisation by authorities are now essential.

We propose a novel geographic risk assessment methodology to improve both red-flagging practices in transaction monitoring by OEs and the prioritisation of growing numbers of STRs for more effective identification, investigation, and prosecution of financial criminal conduct. Designed on the basis of the Financial Action Task Force (FATF)'s conceptualisation of risk, our approach integrates geographic risk considerations derived from objective and verifiable data, mirroring a macro approach discussed recently in the context of National Risk Assessments (Grondona et al. 2025). It builds on the notion that financial secrecy creates a criminogenic environment which enables illicit financial flows (IFFs) and transactions. Not least in the EU's AML regulation 2024/1624 (European Parliament and Council 2024b), secrecy is explicitly recognised as a key enabling factor in illicit finance (Annex III(3)(f)). Everything else equal, the more secretive a transaction (involving sender, recipient, and means of transfer), the higher the risks of illicit activity. The higher the value of the transaction, the bigger its potential harm.

Our methodology for improved geographic risk assessment combines data on the likelihood of an illicit activity to occur with a measure of the scale of harm or damage that would result if it was to occur. To this end, our model focuses on two types of

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

variables that are difficult to manipulate and mostly available in financial transactions as well as STRs: transaction amount and jurisdiction of the sender and the receiver of the money flow. To operationalise the geographic component of this simplified framework, we use the Secrecy Scores (SS) of the Financial Secrecy Index (FSI) (Tax Justice Network 2025) for the approximation of the diverse opportunities for IFFs in a given jurisdiction.

In order to showcase the methodology, we apply it to the FinCEN leaks dataset made available by the International Consortium of Investigative Journalists (ICIJ), including over 18,000 transactions stemming from 534 Suspicious Activity Reports (SARs) (Shiel & Starkman 2020).[1] As the quantitative and qualitative analysis of these results indicate, our proposed risk model adds substantial value to national and regional LEAs. Previous research has shown the same approach can be applied to monitor financial transactions in the context of SWIFT and ISO 20022 wire transfers (Meinzer et al. 2023).

This chapter is organised as follows. Section 3.2 includes a literature review and positions our contribution in the literature. In Section 3.3, we discuss the methodology, data, the model and limitations. Section 3.4 presents the results of applying the model to the empirical dataset of available STRs. Section 3.5 concludes.

3.2 LITERATURE REVIEW AND CONTRIBUTION

Supported by a global system of norms, policy recommendations and standards as well as mutual evaluations of their implementation via peer reviews, a transnational legal order (Halliday & Shaffer 2015) for the prevention of money laundering has been established since the creation of the FATF in 1989. While some elements of this order remain contested and are still in the process of normative settlement (such as beneficial ownership transparency (Ates et al. 2025b)), other elements are firmly established. This chapter contributes to and connects two of those established elements, namely the system of mandatory filing of STRs by OEs from the private sector, and the risk-based approach (RBA) for countering money laundering. We proceed by revisiting relevant debates across criminology, law, economics, and computer science.

3.2.1 *Suspicious Transaction Reports (STR)*

STRs are central to AML and counter-terrorist financing efforts, enabling LEAs to identify potentially illicit activity. Since the FATF's first recommendations in 1990, which required countries to enact suspicious transaction reporting (FATF 1990), STRs have become standard practice. In 2025, FATF Recommendation 20

[1] For our purposes, we consider there is no significant difference between SARs and STRs. Henceforth, we will collectively refer to them as STRs.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

mandates that financial institutions report suspected criminal or terrorist-related funds to FIUs (FATF 2012–2025). However, beyond general requirements like identifying transaction originators and beneficiaries (Rec. 16), global STR formats and content are not harmonised.

Legal scholars have examined the broadening scope of reporting duties (Borlini & Montanaro 2017; Ping 2005) and the lack of comparative research on FIUs and STR practices in Europe (Panevski et al. 2021). Compliance among Designated Non-Financial Businesses and Professions (DNFBPs), such as lawyers and real estate agents, is often weak (Nduka & Sechap 2021; Omar & Johari 2015). While, in some jurisdictions, disclosures may be legally constrained by professional secrecy, low STR submissions from these sectors can mislead authorities about the level of risk. Recent work highlights how data-driven systems influence AML professionals' behaviour in monitoring and red-flagging transactions (Ogbeide et al. 2024).

STR submission processes vary widely, even within the EU. Despite broad use of the goAML software (United Nations n.d.), differences persist in technology, red flags, legal frameworks, and automation. The fourth AML Directive (Directive (EU) 2015/849 or '4AMLD') does not standardise format or content, while other countries across the globe allow STRs to be submitted in paper format (European Parliament and Council 2024a; FATF 2019). Although the latest EU AML package aims to harmonise these elements (European Council 2024), earlier explicit ambitions have been scaled back (European Commission 2021 Article 50).

A key concern in the literature is the exponential growth of STRs, often generating an 'overflow of useless AML information' (Dalla Pellegrina & Masciandaro 2009 p. 932). Defensive over-reporting by OEs, driven by fear of penalties and lack of reward for precision, reduces the effectiveness of STRs (Ross & Hannan 2007 p. 107; Takáts 2007). Though RBA were introduced to curb this trend, STR volumes often keep growing and false positive rates remain high – ranging from 30 per cent to over 95 per cent (Chen et al. 2018 p. 276; Jensen & Iosifidis 2023 p. 8889; Riccardi & Reuter 2024; Richardson et al. 2019).

Scholars emphasise the need for a feedback loop between FIUs and reporting entities to improve STR quality (Ogbeide et al. 2023 p. 9). Currently, entities often lack insight into outcomes of their reports, hindering refinement of detection systems. A robust feedback mechanism would enhance the utility of STRs and enable greater use of artificial intelligence (AI) and machine learning in AML frameworks.

3.2.2 *Geographic Risks in Financial Crime Literature*

The RBA became a cornerstone of AML frameworks following the FATF's 2003 recommendations. With further refinements in 2007 and 2013, it has since become embedded in transnational AML legal frameworks (Financial Action Task Force 2003, 2007, 2013; Ross & Hannan 2007 p. 107). Regulators continue issuing updated

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

guidance on how OEs and LEAs should address IFF risk (European Banking Authority 2021; European Commission 2022; European Union 2023; Financial Action Task Force 2022), and substantial fines have been imposed on OEs when automated red-flagging models failed (Turksen et al. 2024 pp. 373–374).

At the macroeconomic level, the International Monetary Fund (IMF) has employed machine learning and case study analysis to trace abnormal financial flows and assess national vulnerabilities – including around financial secrecy (Jackson et al. 2023). Regulatory impacts on money laundering routes have been documented empirically (e.g. Aldama-Navarrete 2021), and national risk assessments remain a major theme in AML scholarship (Ferwerda & Kleemans 2019; Grondona et al. 2025).

At the micro level, scholars have developed numerous models of AML risk assessments. Ross & Hannan (2007) defined essential conditions for risk-based decision-making to work effectively: shared definitions of risk, a quantifiable model, and feedback loops from outcomes. These principles remain pivotal in legal, criminological, and supervisory analyses. Although some scholars (Bello & Harvey 2017; de Koker 2009) critique FATF's vagueness, we align with those building upon its framework. For example, Savona et al. (2017 pp. 26–27) specify a function of risk consisting of two elements: the probability of an adverse event occurring, and the impact that would result if it did.

Risk models often consider at least three categories of risk, always inclusive of geographic risk (Alexandre & Balsa 2023 p. 2; AUSTRAC & Australian Government 2020; Sathye & Islam 2011 p. 172). FATF's guidance highlights geographic, customer, and product/service risk (Financial Action Task Force 2007 pp. 22–23) and the EU's 2024 AML package further specifies parameters within these categories (European Parliament and Council 2024b, Article 20 and Annex III).

Geographically determined levels of financial secrecy are widely used in both research and administrative practice. For example, Riccardi & Reuter (2024 pp. 341, 348–349) use financial secrecy in their conceptual framework to explain the level of sophistication of money laundering methods. Similarly, the models proposed by Hopkins and Shelton (2019, pp. 67–69), Savona et al. (2017, p. 162) or the research carried out by the Italian Central Bank (Cassetta et al. 2014) conceptualise jurisdictional financial secrecy as drivers of IFFs.

In administrative practice, financial secrecy is acknowledged to facilitate tax evasion (ECORYS 2021), money laundering, and the financing of terrorism (European Commission 2022; EUROPOL 2021; Savona et al. 2017). As the European Commission's 2022 Supra-National Risk Assessment states: 'Anonymity remains a critical vulnerability in the international financial system, [. . .] legal entities and arrangements are valued by criminals for their ability to enhance anonymity and conceal the identity of beneficial owners, as well as a means to carry out their illicit activities, for example by facilitating logistics or transport of illicit goods' (European Commission 2022 p. 10). In the EU, the regulatory

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

environment entering into force in 2027 explicitly requires the new Anti-Money Laundering Authority (AMLA) to issue guidelines defining money laundering (ML) risk factors (Article 32), including 'third countries identified by credible sources or pursuant to acknowledged processes as enabling financial secrecy' (European Parliament and Council 2024b, Annex III(3)(f)).

Empirical research on AML is severely constrained by data access limitations due to confidentiality of police files and STRs (Levi et al. 2018; Reuter & Riccardi 2024 p. 331). Data from OEs can be hard to access too, yet a body of research has been developed including by tapping into the 'pool' of innocent transactions to which red flagging is applied.

Computer science literature discusses technical innovations in red flagging and STR analysis, including through outlier detection, AI and machine learning models, and visualisation strategies (Jensen & Iosifidis 2023; Lebid & Veits 2020; Singh & Best 2019). The features a successful AML data analysis tool for flagging STRs should possess include 'data quality, detection accuracy, scalability, and reaction time' (Chen et al. 2018 p. 248).

Additionally, the literature discusses two persistent problems with accessible data on risk assessment models. First, criminological and legal literature has warned against racial bias and disproportionate exclusion embedded in AI tools (Turksen et al. 2024). In one documented case, ethnic minorities were systematically excluded from banking services by AI systems (Chen et al. 2018 p. 279). These tools can infringe fundamental procedural rights such as the right to a fair trial and the presumption of innocence (Sachoulidou 2023).

A second issue concerns geographic risk indicators themselves. The widespread use of so-called 'blacklists' – like FATF grey/blacklists or the EU's non-cooperative jurisdiction list – often reflects political biases rather than objective data. Research shows that countries with limited geopolitical power, especially from the Global South, are overrepresented on such lists, while powerful nations (e.g. the US) are omitted even though they are essentially displaying the same characteristics as the listed ones (Bello & Harvey 2017; de Koker 2024; Dolar & Shughart 2011; Meinzer 2016; Sharman 2010; Unger 2023). Even advanced systems struggle with concomitant oversimplification. For example, the risk models of the Spanish notary supervisory authority use binary categories such as domestic/foreign or inclusion in official high-risk country list (García Fresno 2022; Ministerio de Hacienda y Función Pública 2023), thereby missing the nuance of secrecy gradients. The European Parliament has noted that EU tax 'blacklists' may be politically motivated rather than being grounded in objective assessments (European Parliament 2023).

Against this background, we argue that a more robust, data-driven alternative is needed. Instead of dichotomous classifications, jurisdictions should be evaluated on a spectrum of financial secrecy, using independent, transparent, and verifiable data. This approach reflects growing consensus across disciplines and aligns with best practices for reducing discriminatory, politically biased, or overly simplistic assessments.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

3.2.3 *Research Gap and Contribution*

Since the publication of the IARM study of 2017 (Savona et al. 2017), a consensus is emerging in the literature on the need of more robust geographic risk assessment based on the levels of financial secrecy in AML. Riccardi and Reuter have conceptualised the AML environment money launderers are facing to a large extent in terms of geographically bound levels of financial secrecy. More specifically, they argue that low levels of banking and corporate transparency, coupled with the absence or weakness of cash regulations and asset recovery policies, attract money launderers, hence increasing the risk of ML (Riccardi & Reuter 2024 pp. 348–349). Yet, they remain silent on a data source or operationalisation of these levels of corporate and banking transparency. It is this gap we propose to fill with our approach.

At the level of computer science, we build on Jensen and Iosifidis who argue that 'banks face two principal data analysis problems in AML: (i) client risk profiling and (ii) suspicious behavior flagging' (Jensen & Iosifidis 2023 p. 8890). While our contribution lies in the second of those categories and more specifically at the transaction level, we argue that our model can be applied by both OE and LEAs. The data processing challenges faced by OE and LEAs are similar not least because the number of STRs continue to grow and for many countries surpass the mark of hundreds of thousands of STRs per year (Vedrenne 2023; Xue & Zhang 2016). The challenges encompass various dimensions, ranging from normative and legal (discrimination) to statistical challenges caused by data features of class imbalance and related challenges (Jensen & Iosifidis 2023). Both need scalable systems with real time processing capabilities that ensure accuracy while keeping a high detection rate. Our approach can be combined with existing statistical inference methods for the detection of crime, with the potential to ultimately reduce the ratio of false positive alarms while increasing STR effectiveness for OE and LEA alike.

We respond directly to calls for integrating transaction monitoring into dynamic risk assessment (Lannoo & Parlour 2021 p. 25) and to calls for a model that can operate with parsimonious data input, as opposed to possibly more complex models which have tended to fail to deliver robust results either because of their lack of transparency or because relevant data inputs have not been available consistently enough across time and space (Hopkins & Shelton 2019 pp. 66–67). The proposed method exploits geographic and transaction volume data found in STRs to produce unambiguous and dynamic prioritisation for further investigations or reporting and equips the OE and LEAs with relevant knowledge to inform their decision-making processes on filing an STR or opening further investigations, respectively. Beyond the technical efficiency of this geographic risk approach, a key operational advantage is its capacity to inform compliance officers and supervisors on the underlying risks related to the regulatory framework in place where the parties to a transaction are established. By drawing on an open-source repository of verifiable legal data,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

relevant information can be made available to investigators as need arises, showing overall scores, broad risk categories, or specific legal analysis. Thus, even without detailed knowledge of the regulatory particularities in each jurisdiction, investigators and OEs should be able to assess geographic risks in any given case and understand the nature of underlying vulnerabilities.

From a behavioural perspective, the proposed methodology hinders strategic manipulation in two ways. First, neither criminals in the case of OEs, nor OEs in the case of LEAs, can anticipate the outcome of their reporting with a view to potentially structure their transactions or filing of STRs with the intention to remain below certain thresholds or alarm levels. As they do not have access to the pool of transactions or STRs in which they are transacting or filing, respectively, they cannot know for certain if a specific transaction would be prioritised as high risk in the dynamic data pool. Second, criminals could decide to transfer activities to jurisdictions with lower Secrecy Scores, yet this would prove self-defeating in the longer term because stronger regulations would greatly increase the risk of detection and prosecution of illicit activity.

In comparison to other risk assessment methods, our approach avoids bias at two different levels. First, the FSI methodology employs a uniform standard across countries to avoid political bias, unlike inconsistent approaches such as the EU Code of Conduct and FATF listings, which often overlook high-risk financial activities in geopolitical allies (e.g. the US and Luxembourg) while disproportionately targeting adversarial jurisdictions (e.g. Iran and North Korea), which are routinely blacklisted (FATF-GAFI 2003). Such biases, including documented discrimination against Global South countries (Dean & Waris 2021), are heavily amplified when the output of risk assessments is a binary classification (high risk vs. low risk). The proposed approach assigns values from 0 (most transparent) to 100 (most secretive), enabling a more nuanced evaluation of secrecy risks (Janský et al. 2022). Second, the model's orientation toward regulatory context, rather than sender or recipient personal characteristics, ensures that assessments remain non-discriminatory. Scoring systems often used by OEs and LEAs run the risk of embedding bias through profiling, potentially resulting in systemic discrimination (Sciurba 2018).

Finally, the proposed geographic risk methodology can be considered forward-looking for different reasons. On the one hand, the evaluation of Secrecy Indicators using the 'weakest link' approach highlights loopholes available in jurisdictions even if these can be considered dormant, in the sense that there is no indication yet that they have been exploited by criminals. The capacity to account for potential (future) exploitation of regulatory loopholes provides a clear advantage over statistical methods that infer risks only on the basis of past criminal activity (see Lebid & Veits 2020). On the other hand, many FSI indicators have set early benchmarks that later influenced global standards. Indeed, while FATF recommendations are widely viewed as global AML standards, they emerge from slow-moving institutional

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

consensus, often shaped by self-regulatory ideology and the disproportionate lobbying power of certain member states, raising concerns about neutrality, effectiveness, and the influence of geopolitical interests. The FSI's ambitious benchmarks ensure that gaps are highlighted, even when media attention or policy priorities have not yet driven the establishment of stronger global regulations. For example, requiring beneficial owners of legal entities to be registered with a public authority – rather than with a private intermediary – has been an FSI standard since its inception in 2009 and only in recent years has been adopted in the EU and beyond (Ates et al. 2025b).

The proposed model thus intends to complement existing systems equipping both LEAs and OEs with a dynamic risk-assessment methodology that may serve as a basis for further analysis or be used as a cross-checking tool to make sure no high-risk transaction or STR is disregarded. The following section explains in detail how our assessment works and how it is applied to a dataset of STRs.

3.3 Modelling Geographic Risk in Financial Transactions

We estimate the geographic risk inherent to a transaction by combining three types of data, two of which are included in most transaction reports, including STRs: the amount as well as the jurisdiction of the sender/receiver of the transaction. We enrich this data with the levels of financial secrecy of the jurisdictions concerned in the transactions to arrive at a relative measure of risk.

3.3.1 *Data*

3.3.1.1 Suspicious Transaction Report (STR) Data

Legal research on STRs undertaken in the TRACE project compared reporting requirements across EU member states and evaluated the role of STR/SARs within AML investigative processes. Yet attempts to obtain anonymised STR data from EU authorities yielded a relatively small sample of twenty-one STRs from two EU member states. While this sample provided useful insights on STR reporting differences and opportunities for harmonisation, it was insufficient to showcase the effectiveness of our geographic risk assessment in providing a simple way to evaluate risk across large datasets and ultimately improve the allocation of investigative resources. For this reason, we use an extensive dataset of 534 STRs that includes more than 18,000 underlying transactions, made available by the ICIJ following the FinCEN leaks (ICIJ 2020).

The Financial Crimes Enforcement Network (FinCEN) is the FIU of the United States Treasury Department. It is responsible for collecting, analysing, and disseminating financial information related to investigations of illicit finance, including ML and terrorist financing (TF). In order to better exploit the STRs data that is filed

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

by reporting entities, FinCEN analysis of this data also includes the identification of emerging trends and techniques related to ML and other financial crimes, as specified in Article 31 USC 310(b)(2)(C) (US Congress 2024). This allows FinCEN to enhance its knowledge of methodologies, typologies, geographic patterns of activity, and systemic weaknesses pertaining to ML and TF (FATF-GAFI 2016 pp. 60–62). The analytical work is primarily focused on intricate cases where LEAs require support in identifying multiple individuals involved, mapping out criminal financial activities across extensive geographical regions, and establishing international connections that may not be immediately evident during initial investigations. FinCEN's analysts also generate threat assessments, industry reports, and technical guides that offer insights into financial transaction mechanisms (FATF-GAFI 2016). According to a FinCEN report published in 2024, the number of SARs filed by reporting entities to FinCEN in 2023 was approximately 4.6 million (FinCEN 2024).

The ICIJ investigation of the leaked FinCEN files was published in September 2020 and exposed vast amounts illicit transfers by banks. The investigation was based on a trove of classified documents, obtained and shared by BuzzFeed News. The documents included more than 2,100 SARs filed by global banks with FinCEN. This unprecedented data leak evidenced the movement of over USD 2 trillion in potentially illicit payments between 1999 and 2017, all of which were flagged by the banks themselves (ICIJ 2020). The leaked documents include numerous spreadsheets detailing the activities of financial institutions with clients under suspicion across more than 170 countries and territories.

Despite the various tools implemented by FinCEN to monitor typologies and geographic patterns of activity, the ICIJ found that in half of the FinCEN files reports, information was missing about at least one or more entities behind the transactions (ICIJ 2020). The data used for this study is a sub-sample of 534 SARs which represents approximately 25 per cent of the 2,100 SARs included in the leaked records. The sub-sample corresponds to the transactions for which ICIJ journalists were able to identify sufficient details on both the originator and beneficiary banks (ICIJ 2020) and represents approximately USD 35 billion (out of more than USD 2 trillion worth of transactions in the leaked files), or about 1.75 per cent. In our view, the fact that only a minor part of the leaked STRs actually included data on the countries from which the transactions were sent and in which they were received – let alone the actual identity of the originators and beneficiaries – provides a clear indication for a need to systematise and harmonise the way STRs are filed.

In the EU, the evolving regulatory environment exemplifies international initiatives to harmonise STR reporting. With regards to geographic information in STRs (i.e. the location of the transaction's sender and recipient), most reports accessed for this chapter present the information in a (semi-)standardised format. As mentioned above, we expect that minimal reporting requirements related to sender and recipient jurisdiction will be implemented in the near future, resulting from the interplay

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

between AMLR 2024/1620 (Articles 1(3), 5(5)(j) and Article 50) and AMLR 2024/1624 (Article 69) (European Parliament and Council 2024b 2024c). Geographical locations of sender and recipient are not only superior to other variables in terms of data availability, but they also represent transaction features that are hard to obfuscate and usually directly verifiable by OE and supervisors alike.

While certain jurisdictions may be ahead in terms of STR reporting systems and analysis, we expect that increased harmonisation at regional or global levels will gradually allow more systematic and evidence-based assessment of cross-border ML risks. Importantly, consolidation of STR data from multiple jurisdictions should clear the way for comprehensive research on anonymised STR data.

3.3.1.2 Financial Secrecy Index (FSI) Data

Our analysis incorporates data on financial secrecy laws and practice across multiple jurisdictions, drawing from official reports, datasets from international organisations and original legal assessments. Wherever feasible, the scoring incorporates the results of tests on how the regulatory framework is operating in practice. This data forms the basis of the FSI 2025 (Tax Justice Network 2025).

Since its inception in 2009, the FSI methodology has undergone eight revisions. The 2025 edition categorises twenty equally weighted Secrecy Indicators (SI) into four key dimensions to assess jurisdictional vulnerabilities to financial crime (see Table 3.1). Ownership registration (Indicators 1–6) evaluates banking secrecy, anonymous trusts/foundations, bearer shares and shell companies, real estate, and high-value assets, where absence of ownership registration enables exploitation for criminal purposes. Legal entity transparency (Indicators 7–11) focuses on corporate structures, measuring vulnerabilities from opaque limited liability partnerships, undisclosed company ownership, non-public accounts, and inadequate country-by-country reporting or Legal Entity Identifier (LEI) use – gaps that facilitate large-scale tax evasion and other financial crimes. Tax and regulatory integrity (Indicators 12–16) assesses enforcement weaknesses, including lax tax avoidance reporting, golden visa schemes, problematic personal and capital income tax policies, and non-disclosure of tax rulings or extractive contracts, which collectively foster tax avoidance and corruption. International cooperation (Indicators 17–20) scrutinises the adherence to FATF standards, automatic tax data exchange (CRS/MCAA), and treaty ratifications that provide concrete legal avenues for cooperation on financial crime investigation and prosecution. Together, these indicators provide a systematic, evidence-based approach to quantify how jurisdictional loopholes amplify vulnerabilities to IFFs (Tax Justice Network 2025).

The geographic risk data within Secrecy Scores builds on economic and criminological research, analysing behavioural shifts following regulatory changes and evolving *modi operandi* of financial crime. The selection of risk indicators (regulatory characteristics that affect the likelihood that activities in a jurisdiction are

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

TABLE 3.1 *The twenty financial secrecy indicators underpinning the secrecy score*

1 Asset and ownership registration	Legal entity transparency	Integrity of tax and financial regulation	International standards and cooperation
1 Banking secrecy	7 Transparency of partnerships with limited liability	12 Tax compliance focus	17 Anti-money laundering
2 Beneficial ownership of trusts	8 Transparency of company ownership	13 Golden visas	18 Automatic exchange of information
3 Beneficial ownership of foundations	9 Transparency of company accounts	14 Foreign investment income	19 Exchange of information upon request
4 Beneficial ownership of companies	10 Public country-by-country reporting	15 Public statistics	20 International legal cooperation
5 Freeports ownership	11 Legal entity identifiers	16 Tax rulings and extractive industries' contracts	
6 Real estate ownership			

exploited for financial crime) has followed a combined inductive/deductive process. On the one hand, we reviewed databases with comparative data on country regulations (e.g. FATF, OECD, UN, IMF, IBFD, etc.) to determine whether any readily available data could be used to assess secrecy risks. For instance, we integrate FATF Recommendation ratings into three different indicators, in relation to banks and crypto intermediaries' ownership-registration obligations (SI 1) and more generally AML regulations (SI 17) and effectiveness of international cooperation (SI 20). Thus, an inductive process allowed for the identification of various risk components. On the other hand, expert publications from international organisations (IO), academia, and civil society were reviewed in order to determine what additional regulatory characteristics could be included in the risk assessment framework. For this purpose, we considered not only the direct relevance to the underlying threat (ML, TF, fraud, tax abuse), but also the available resources to undertake comparative research across jurisdictions. An important motivation to undertake this additional research is that FATF comparative assessments (ratings) are not specific enough to identify concrete regulatory loopholes, and often disregard vulnerabilities on the basis of subjective, non-verifiable assessments. This deductive process yields additional risk components that are combined with other relevant data from existing sources.

An important feature of FSI's Secrecy Scores is their resilience and methodological accountability. Since 2009, the FSI has been updated biennially, with all

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

indicators revised simultaneously to reflect regulatory developments. Beginning in 2025, the FSI has transitioned to a rolling update system, publishing revised data for selected indicators every few months within a three-year cycle. The new system ensures that any regulatory changes flagged by jurisdictions in annual consultation exercises are integrated, following a strict verification process. This shift to rolling updates enables the index to incorporate regulatory changes as they emerge, offering a more dynamic and timely assessment of jurisdictions' roles in financial secrecy and global tax abuse (Meinzer & Harari 2023). This is a significant advantage over FATF evaluations, some of which have taken almost a decade to reassess like Luxembourg (FATF n.d.) and the United States (FATF 2024). Thus, proposed geographic risk data secures resilience through continuous updates, and ensures accountability by transparently identifying all underlying sources and giving jurisdictions the opportunity to enrich or rectify assessments.

3.3.2 *Methodology*

We develop our risk assessment method on the basis that risk is a combination of the potential impact of an occurrence of financial crime, and the likelihood for that impact to materialise (Savona et al. 2017 pp. 26–28). Building on the FATF risk assessment framework (FATF 2013), we conceptualise risk as a combination of the probability or likelihood of financial crime (derived from underlying threats and vulnerabilities) with its potential impact (Savona et al. 2017). As for the likelihood of ML and other financial crimes to occur, we use aggregate data of secrecy features at the jurisdiction level that act as proxies of relative threats and/or vulnerabilities. The following example illustrates this conceptual framework.

Consider a corporate officer approving a transaction as a payment to a company supplier or service provider established in another jurisdiction. If such jurisdiction requires systematic registration, verification and online publication of the beneficial owners of legal entities established therein, the likelihood that the corporate officer is embezzling funds would be low, insofar as it is quite simple for anyone to check whether the corporate officer is a beneficial owner of the recipient company, and criminal activity would thus be easy to detect. If, however, the recipient jurisdiction does not require beneficial ownership (BO) registration, the likelihood that the individual embezzles funds is higher, given that the obfuscation of effective ownership and control can disguise the transaction as a legitimate payment to an independent third party (Cardao-Pito 2022). In the two situations, the potential impact of illicit activity would be the same transaction amount. Thus, *ceteris paribus*, combining the likelihood of illicit activity with its impact, the risk of the considered transaction will be higher in the latter situation. As we want to aim for a prioritisation of STRs, rather than for an estimate of expected damage, our numerical representations of risk are not meaningful in absolute terms. Rather, they are useful only insofar as they convey a relative understanding of risks among different occurrences.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Aligned with the two conceptual pillars, we combine two types of measures: (i) a quantitative measure of the economic value at stake in the assessed transaction(s), and (ii) a quantified measure of the opportunities for criminal activity offered by secrecy jurisdictions. Our approach produces a single and clearly defined risk score for each transaction on the basis of the widely established knowledge that IFFs follow weak regulations and secrecy, that is that large transactions between jurisdictions where money can be easily hidden have the highest IFF risk (Aldama-Navarrete 2021; Boyer & Kempf 2020; Cobham et al. 2015; Houston et al. 2012; Janský et al. 2022).

From a methodological perspective, optimal STR risk assessment should aim to integrate any relevant indicator and account for as many different types of risk as possible. However, the lack of relevant data across jurisdictions can make STRs difficult to compare on the basis of more complex frameworks. We claim that at a minimum, STR-based risk assessment should take into account the opportunities available in originator and recipient jurisdictions to hide or obfuscate the true nature of underlying economic activity. The present approach minimises STR data preconditions (amount, origin, destination), to then fully develop secrecy risks on the basis of jurisdictions' regulatory features.

3.3.3 *Risk Assessment Model*

Based on the determinations outlined above, we start with the following conceptualisation: *Risk=Likelihood x Impact*

Where:

- *Likelihood* is a function of threats and vulnerabilities, based on the opportunities of regulatory arbitrage allowed by financial secrecy.
- *Impact* is a function of the transaction volume recorded for an STR.

The next relevant definitions for our model concern these two functions, that is, the exact specification of Likelihood (Threat & Vulnerabilities) and Impact (transaction volume). We base these definitions on two considerations. First, we do not aim for an actual quantification of the expected damage, but only for an estimate that allows us to prioritise, that is, rank STRs according to the risk inherent in the reported transactions. Therefore, while the relative Likelihood and Impact of an STR should be commensurate across STRs, the resulting risk value does not need to have an economic interpretation. Second, the scaling of Likelihood and Impact needs to be such that both concepts contribute adequately to the overall risk score, without one of them entirely determining an STR's risk ranking. In this sense, transaction data is known to be highly right-skewed, with the vast majority of transactions being of relatively low value, and only a few transactions take very high values.

As shown in Figure 3.1, this skewing is apparent in the STRs from the FinCEN files. A simple product of our measures of Likelihood and Impact would thus assign

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

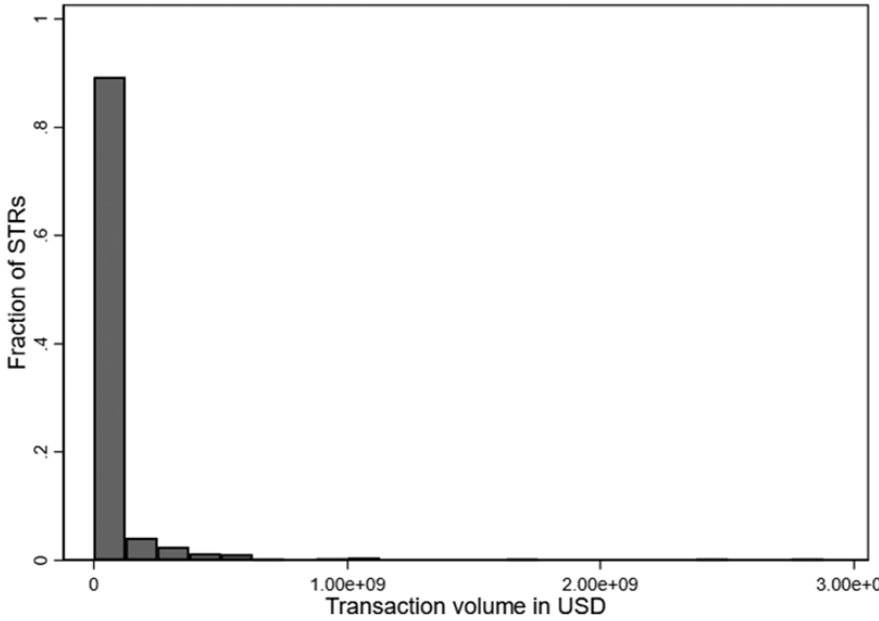


FIGURE 3.1 Distribution of transaction volumes in the FinCEN leaks dataset.

disproportional weight to large transactions, rendering the secrecy information irrelevant. To adjust for this pattern, we cube our likelihood measure and take the cube root of the transaction volume. This aggregation form has been reviewed by a study of the European Commission's Joint Research Center (JRC) (Becker & Saisana 2018). A useful alternative to the cube root function applied to transaction volumes is the logarithm function. For the model presented below, using the suggested cube root or the logarithm of transaction volume does not change the risk assessment of top-ranked transactions.

$$Risk = \left(\frac{SS_A + SS_B}{2}\right)^3 \times \sqrt[3]{transaction\ volume}$$

In order to assess the risk of a transaction from jurisdiction A to jurisdiction B, we determine the likelihood of illicit activity on the basis of the average of Secrecy Scores for the two jurisdictions involved. That average is then transformed through the cube function to derive the likelihood of illicit activity.

In our dataset, most STRs contain multiple transactions. This can be explained by the fact that a pattern of transactions is considered suspicious, rather than a specific unique transaction, and the obliged entity submits an STR to the FIU which includes all transactions considered potentially tainted by illicit activity. In order

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

to adjust our risk model to such situations, we calculate a weighted average of Secrecy Scores.

$$Likelihood = \left(\frac{\sum_i^n \left(\frac{SS_{Sender(i)} + SS_{Recipient(i)}}{2} \right) \times V_i}{\sum_i^n V_i} \right)^3$$

Where:

- n is the total number of transactions included within a STR report
- i designates sequentially each of the transactions in the STR report
- Vi corresponds to the transaction volume of the i^{th} transaction
- $SS_{Sender(i)}$ reflects the Secrecy Score of the sender jurisdiction as applicable in the i^{th} transaction
- $SS_{Recipient(i)}$ reflects the Secrecy Score of the recipient jurisdiction as applicable in the i^{th} transaction

Thus, we can formalise a given STR's geographic risk with the following equation:

$$\text{Risk} = \left(\frac{\sum_i^n \left(\frac{SS_{Sender(i)} + SS_{Recipient(i)}}{2} \right) \times V_i}{\sum_i^n V_i} \right)^3 \times \sqrt[3]{\sum_i^n V_i}$$

In transactions where sender or receiver country information are missing, adjustments could be made to seamlessly include those in the model. For example, country-specific cash regulation scores could be used in case of cash deposits/withdrawals and for crypto-wallet senders and recipients, maximum secrecy could be assumed. This was not needed in the case of the FinCEN data because it lacks cash or cryptocurrency details.

3.3.4 *Limitations*

Despite the various advantages outlined above, the proposed geographic risk model is affected by several limitations.

First, some of the ML techniques relying on new and disruptive technologies can be effectively assessed with the proposed model of geographic risk assessment to the extent that they make use of front companies or bank accounts at some stage of the laundering process, such as 'transaction laundering' (Akartuna et al. 2023 p. 634). However, others prove more elusive to our approach since they lack a clearcut territorial 'location' for meaningful geographical risk attribution and necessitate further conceptual exploration and innovation for seamless integration into a baseline risk assessment model. For example, situations when a company established under the laws of country A has an account in country B, and carries on

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

a transaction with such account, both jurisdictions would be relevant for risk assessment. Optimally, standardised STR data would identify both jurisdictions, and risk indicators would account for threats and vulnerabilities alternatively with respect to country A (e.g. ownership registration) or B (e.g. banking-related AML regulations).

Second, our approach does not claim that automated geographic risk assessment methods are sufficient to identify the riskiest transactions, nor that human analysis of the facts and circumstances of each STR is redundant. Instead, the proposed method is conceived as complementary with other risk-assessment methods, notably those that take into account transaction features in relation to relevant parties' previous behaviour or expected behaviour in the context of transaction patterns across relevant economic sectors. There will always be an important for human agency in the design and evaluation of different risk-assessment outputs and techniques, and expert knowledge will continue to be particularly relevant in situations with potentially far-reaching legal consequences (Ogbeide et al. 2023 pp. 2–3).

Third, the proposed approach is focused on ML but may not accurately represent risks related to TF activities (Savona et al. 2017 pp. 26, 168). This is because in our model we approximate the harm or impact based on a quantitative monetary value, which does not capture the harm resulting from terrorist activities or other concrete predicate offences. Yet, in the realm of financial crimes, it is difficult or impossible to assess the underlying impact of a crime beyond the amount involved. Because all sorts of criminal actors use very similar financial secrecy tools, it can be very difficult to assess 'ex-ante' whether a given amount of funds results from relatively mild criminal activity (such as tax evasion) or from a particularly heinous type of crime (trafficking in human beings). Provided that standardised STR data can identify suspected predicate offences, FIUs may further develop risk-assessment models assigning different weights to transactions suspected of diverse predicate offences.

Finally, the effectiveness of the proposed method in identifying STRs that are relatively more useful in the investigation and prosecution of financial crimes could not be tested due to a lack of data on STR outcomes. The ultimate goal of any STR-based risk-assessment technique would be to single-out reports that are more likely to initiate a successful investigation or contribute to an existing one. This is what Europol refers as STR 'conversion': the fact that an STR filed by an obliged entity is further exploited by relevant authorities in the fight against financial crime (EUROPOL 2017 pp. 29–31). Without comprehensive analysis of large-scale STR datasets including the information on which reports have led to a criminal conviction, or have otherwise supported (ongoing) investigations, any risk analysis tool is arguably unable to demonstrate its effectiveness. Aiming to increase the historically low rate of STR conversion (EUROPOL 2017), international cooperation frameworks should ensure that conversion data is closely monitored in cross-border scenarios, and that comprehensive, anonymised, STR datasets are made available for academic research.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

3.4 RESULTS

Our model is designed for situations where so many different STRs need to be assessed that a manual prioritisation becomes overwhelming. In the following, we illustrate that our model can easily be applied to a large dataset, namely to all available STRs.

Table 3.2 presents the 15 STRs that have been ranked highest by our model out of the 534 STRs leaked in the FinCEN files. The large number of senders and recipients reported for most STRs reveals the high degree of complexity in the STR data of the FinCEN files. While Table 3.2 becomes close to unreadable due to complexity – even though it only includes the most relevant data fields, a slightly adapted version of our analysis[2] allows us to gain overview of the countries that contributed most to the IFF risk in the STRs from the FinCEN Files. As shown in Figure 3.2, transactions originating from or destined for Russia account for the largest share of overall risk (13.7 per cent), followed by those involving Latvia (13.1 per cent) and Switzerland (11.7 per cent).

The figure above illustrates the outputs that can be derived from a comprehensive geographic risk methodology. These outputs can not only be monitored in real time and allow the identification of the largest geographic risk exposures for further investigations or targeted supervisory measures, but also provide valuable input for National Risk Assessments (Grondona et al. 2025).

3.5 CONCLUSION AND POLICY RECOMMENDATIONS

Combating IFFs requires continuous innovation in AML methodologies, particularly as criminals exploit regulatory asymmetries across jurisdictions. This chapter contributes to this effort by developing a dynamic, evidence-based framework for geographic risk assessment that addresses critical gaps in current AML practices. Our approach builds on two decades of risk-based AML frameworks while challenging the limitations of politicised 'blacklisting'. By integrating minimal STR data with SI, we provide a scalable, transparent, and bias-resistant tool that enhances the detection and prioritisation of high-risk cross-border transactions. Unlike retrospective models that flag risks based on past criminal activity, our framework proactively identifies vulnerabilities in financial systems using the 'weakest link' approach. The FSI's rolling updates ensure that regulatory changes are promptly reflected, offering a dynamic alternative to slow-moving FATF evaluations. This forward-looking approach is critical for disrupting ML networks before they exploit weak regulations or enforcement.

[2] To estimate country-level risk contributions, we begin by calculating the risk for each individual transaction rather than for each STR, since a single STR can include multiple transactions. We then aggregate these transaction-level risks by summing all contributions associated with each country and report the country's contribution to overall risk.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

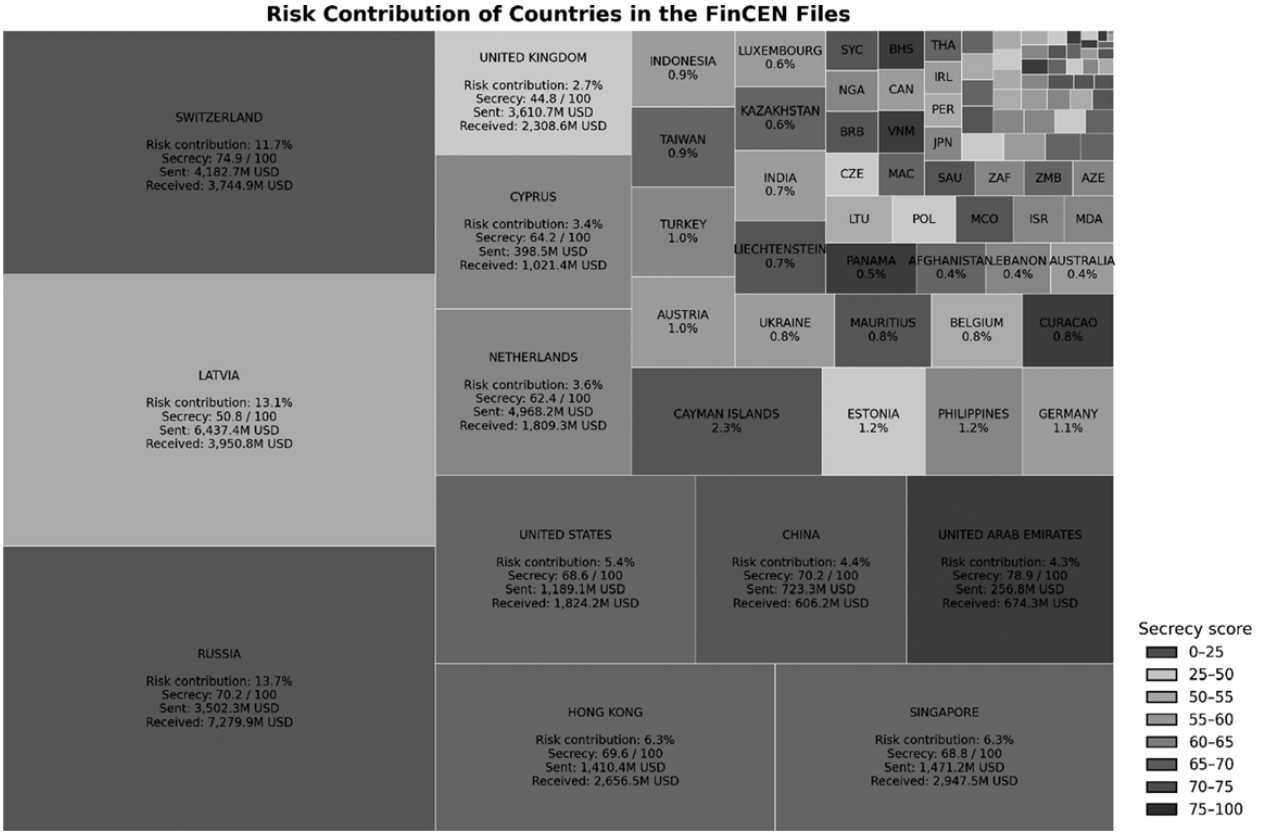


FIGURE 3.2 Risk contribution of different countries in the FinCEN files.

TABLE 3.2 *Priority ranking of STRs in the FinCEN files*

Rank	STR Ref.	ISO sender	Secrecy Sender	ISO recipient	Secrecy Recipient	Secrecy STR	Volume (in US$)	Risk	Risk Contribution	Rank log model
1	2748	BEL, CHE, CYP (5), GBR (7), NLD, RUS (42), USA (11)	63	RUS (57), CHE (5), CYP (2), GBR (4)	70	66	2,878,948,864	416056000	1.17	4
2	2912	CYM (18), GBR (3), HKG (3)	63	HKG (6), USA (12), CYM (6)	72	67	1,658,486,016	357147904	1.00	7
3	2778	CHE (2), GBR, MCO (3), USA (2)	70	CHE (2), SGP (6)	70	70	1,070,848,064	353734144	0.99	2
4	2713	CHE (1), GBR (2), RUS (3)	73	USA (1), CHE (1), MUS (2), GBR (2)	67	70	953,490,048	333647968	0.94	6
5	3670	HKG (2), SGP	69	CHE, SGP (2)	70	70	921,257,600	332390272	0.93	5
6	2338	CHE (5), RUS (121), USA (12)	73	RUS (24), CHE (8), CYP (24), JPN (10), TUR (64), USA (8)	70	72	657,935,296	321726528	0.90	3
7	2266	CHE (12)	75	AUT, CHE (6), RUS (4), USA (1)	75	75	363,403,488	298272224	0.84	1
8	2729	CHE (5), CYP (6), RUS (7), USA	72	CHE (4), LTU, RUS (13), USA	72	72	274,660,960	246020496	0.69	8
9	2704	LVA (38), NLD (23)	57	LVA (23), NLD (38)	57	57	2,400,391,936	243103472	0.68	52
10	2859	LVA (8), RUS (2)	54	CHE (4), RUS (4), LVA (2)	69	61	1,094,978,432	235926608	0.66	30
11	3032	CYM, IRL, LUX, USA (7)	67	CYM (4), RUS, USA (5)	70	69	382,592,224	234950784	0.66	12
12	2322	CYP, GBR, MUS (4)	64	MUS (5), CYP	70	67	456,000,000	229099968	0.64	15
13	4069	CHN, HKG (4), SGP, THA	69	CHE, HKG (2), SGP (3), TWN	70	70	297,866,656	227654992	0.64	10
14	3789	SGP (14)	69	HKG (2), IND (4), SGP (8)	59	64	525,626,368	212822080	0.60	27
15	2380	CYP (4), NLD, RUS (12)	69	CYP (3), NLD (2), RUS (11), USA	68	69	258,861,840	205861328	0.58	16

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Results highlight the ability to flag a reduced number of complex STRs often involving tens of underlying cross-border transactions, through the combination of transaction amounts and geographic regulatory data. We derive a calculation of risk associated with individual jurisdictions in the FinCEN dataset to map out broader secrecy risk exposures: Russia (13.7 per cent), Latvia (13.1 per cent), and Switzerland (11.7 per cent) are found to channel the most risk.

While geographic risk indicator selection and weighting is always open to debate, the FSI proposes a transparent methodology that integrates a variety of concrete regulatory characteristics. Availability of additional or alternative comparative data on financial regulation across a wide number of jurisdictions can allow expansion or adjustment of risk indicators, for instance, focusing on a specific type of ML (e.g. through real estate or high-value assets). Given appropriate resources and political will, methodologies such as the one presented in this chapter can allow targeted reduction of cross-border ML risks across specific categories of OEs. In the EU, expected but uncertain harmonisation of STR reporting and analysis may pave the way for robust, evidence-based, geographic risk assessment.

The implementation of a simple benchmark for STR-based risk assessments can help establish a minimum standard ensuring that no STRs above a certain threshold of risk are disregarded from thorough analysis. Further developments of the proposed risk assessment model could integrate non-public LEA data and calibrate risk indicators to maximise quantifiable policy goals (such as convictions or criminal funds recovered). This requires meticulous record keeping and monitoring of case developments, to ensure that the outcomes or use of each STR are systematically recorded, especially in cross-border scenarios. Furthermore, any successfully prosecuted financial crime case that did not trigger STR should also integrate tainted transactions into a dataset for risk model calibration. Arguably, a comprehensive evaluation of the effectiveness of current STR frameworks cannot be undertaken without analysing a large enough random sample of transactions that were not flagged by OEs. With DNFBPs and Virtual Asset Service Providers (VASPs) repeatedly showcased in vast financial crime cases, the extent of illicit activity in these sectors is a 'known unknown'. We shall question the effectiveness of STR frameworks in contexts where OEs are highly conflicted (business opportunity vs. STR) or directly controlled by criminal interests. In this sense, the development of mandatory transaction reporting systems to complement or replace STRs would be necessary.

In conclusion, this chapter underscores that combating financial crime requires not just technological innovation but also a commitment to transparency and equity in regulatory enforcement. By replacing opaque, politicised 'blacklists' with verifiable secrecy metrics, our framework advances a more just and effective AML ecosystem. The road ahead demands collaboration across academia, industry, and policy-, and lawmakers to refine risk tools, close data gaps, and ultimately disrupt the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

financial architectures that enable IFFs. The promise of this approach lies not only in its analytical rigour but in its potential to reshape AML into a system that is as adaptive and resilient as the threats it seeks to counter.

REFERENCES

Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2023) The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. *Security Journal*, 36, pp.615–650. https://doi.org/10.1057/s41284-022-00356-z (Accessed 9 September 2025).

Aldama-Navarrete, D. (2021) Dark banking? Banks and illicit deposit flows, Federal Reserve Bank of Richmond. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811752 (Accessed 8 July 2025).

Alexandre, C. R., & Balsa, J. (2023) Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, **217**, 119500.

Ates, L., Knobel, A., Lorenzo, F., & Meinzer, M. (2025a) Competition and complementarity of EU and FATF beneficial ownership transparency orders. In I. J. Mosquera Valderrama, F. Heitmüller, J. Chaisse, & A. Christians, eds., *Redefining Global Governance*, Cham: Springer Nature Switzerland, pp.85–96.

Ates, L., Knobel, A., Lorenzo, F., & Meinzer, M. (2025b) The transnational legal ordering of beneficial ownership registration. *Transnational Legal Theory*, **16**, 451–476. www.tandfonline.com/doi/abs/10.1080/20414005.2025.2471184 (Accessed 8 July 2025).

AUSTRAC & Australian Government (2020) *Assessing ML-TF Risk*. www.austrac.gov.au/sites/default/files/2020-08/AUSTRAC%20Insights%20-%20Assessing%20-ML-TF%20Risk.pdf (Accessed 8 July 2025).

Becker, W., & Saisana, M. (2018) The JRC Statistical Audit of the Financial Secrecy Index 2018, Joint Research Centre of the European Commission. https://knowledge4policy.ec.europa.eu/sites/default/files/jrc_statistical_audit_of_the_financial_secrecy_index_2018.pdf (Accessed 9 September 2025).

Bello, A. U., & Harvey, J. (2017) From a risk-based to an uncertainty-based approach to anti-money laundering compliance. *Security Journal*, **30**(1), 24–38.

Borlini, L., & Montanaro, F. (2017) The evolution of the EU law against criminal finance: the 'hardening' of FATF standards within the EU. *Georgetown Journal of International Law*, **48** (4), 1009–1062.

Boyer, P. C., & Kempf, H. (2020) Regulatory arbitrage and the efficiency of banking regulation. *Journal of Financial Intermediation*, **41**, 100765.

Cardao-Pito, T. (2022) An embezzler test for norms, standards and regulations. *Journal of Financial Crime*, **29**(3), 878–889.

Cassetta, A., Pauselli, C., Rizzica, L., & Tonello, M. (2014) *Exploring Flows to Tax Havens Through Means of a Gravity Model: Evidence from Italy* (No. 236), Rome. https://papers.ssrn.com/abstract=2575647 (Accessed 8 July 2025).

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018) Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, **57**(2), 245–285.

Cobham, A., Janský, P., & Meinzer, M. (2015) The Financial Secrecy Index: shedding new light on the geography of secrecy. *Economic Geography*, **91**(3), 281–303.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Cusack, J. (2022, January 2) Financial Crime Bank Fines in the 21st Century. *Financial Crime News*. http://thefinancialcrimenews.com/financial-crime-bank-fines-in-the-21st-century-by-fcn/ (Accessed 8 July 2025).

Dalla Pellegrina, L., & Masciandaro, D. (2009) The risk-based approach in the new European anti-money laundering legislation: a law and economics view. *Review of Law and Economics*, **5**(2), 931–952.

de Koker, L. (2009) Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance. *Journal of Financial Crime*, **16**(4), 334–352.

de Koker, L. (2024) Editorial: FATF greylisting: time to revisit the approach. *Journal of Money Laundering Control*, **27**(4), 621–624.

Dean, S., & Waris, A. (2021) Ten truths about tax havens: inclusion and the 'Liberia' problem. *Emory Law Journal*, **70**(7). https://papers.ssrn.com/abstract=3822421 (Accessed 8 July 2025).

Dolar, B., & Shughart, W. F. (2011) Enforcement of the USA Patriot Act's anti-money laundering provisions: have regulators followed a risk-based approach? *Global Finance Journal*, **22**(1), 19–31.

ECORYS (2021) *Monitoring the amount of wealth hidden by individuals in international financial centres and impact of recent internationally agreed standards on tax transparency on the fight against tax evasion*, Brussels: European Commission DG TAXUD.

European Banking Authority (2021) Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ('The ML/TF Risk Factors Guidelines') under Articles 17 and 18(4) of Directive (EU) 2015/84. www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20–ML%20TF%20Risk%20Factors.pdf (Accessed 8 July 2025).

European Commission (2021) Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, Pub. L. No. COM/2021/420 final (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0420 (Accessed 8 July 2025).

European Commission (2022, October 27) Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554 (Accessed 8 July 2025).

European Council (2024, May 30) Anti-money laundering: Council adopts package of rules [Press Release]. www.consilium.europa.eu/en/press/press-releases/2024/05/30/anti-money-laundering-council-adopts-package-of-rules/ (Accessed 8 July 2025).

European Parliament. (2023). *Lessons learnt from the Pandora Papers and other revelations* (Resolution No. P9_TA (2023)0249), Brussels, Belgium. www.europarl.europa.eu/doceo/document/TA-9-2023-0249_EN.pdf (Accessed 8 July 2025).

European Parliament and Council. (2024a) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (Text with EEA relevance), 2015/849. http://data.europa.eu/eli/dir/2015/849/2021-06-30/eng (Accessed 8 July 2025).

European Parliament and Council (2024b) Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

system for the purposes of money laundering or terrorist financing (Text with EEA relevance). http://data.europa.eu/eli/reg/2024/1624/oj/eng (Accessed 9 September 2025).
European Parliament and Council (2024c) Regulation (EU) 2024/1620 of the European Parliament and of the Council of 31 May 2024 establishing the Authority for Anti-Money Laundering and Countering the Financing of Terrorism and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (Text with EEA relevance). https://eur-lex.europa.eu/eli/reg/2024/1620/oj (Accessed 8 July 2025).
European Union (2023) High risk third countries and the international context content of anti-money laundering and countering the financing of terrorism. https://finance.ec.europa.eu/financial-crime/high-risk-third-countries-and-international-context-content-anti-money-laundering-and-countering_en (Accessed 23 April 2026).
EUROPOL (2017) *From Suspicion to Action: Converting financial intelligence into greater operational impact*, EU. www.europol.europa.eu/cms/sites/default/files/documents/ql-01-17-932-en-c_pf_final.pdf (Accessed 8 July 2025).
EUROPOL (2021) *Shadow Money: The International Networks of Illicit Finance*, EU. www.europol.europa.eu/cms/sites/default/files/documents/Shadow%20money%20%E2%80%93%20the%20international%20networks%20of%20illicit%20finance_PUBLIC_0.pdf (Accessed 8 July 2025).
FATF (1990) *The Forty Recommendations of the Financial Action Task Force on Money Laundering*, Paris: Financial Action Task Force (FATF). www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-states-2016.html (Accessed 8 July 2025).
FATF (2012) *The FATF Recommendations: International standards on combating money laundering and the financing of terrorism & proliferation*, Paris, France: Financial Action Task Force (FATF). www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (Accessed 8 July 2025).
FATF (2013) *National Money Laundering and Terrorist Financing Risk Assessment*, Financial Action Task Force (FATF). www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf (Accessed 8 July 2025).
FATF (2019) Anti-money laundering and counter-terrorist financing measures Turkey Mutual Evaluation Report. www.fatf-gafi.org/content/dam/fatf-gafi/mer/Mutual-Evaluation-Report-Turkey-2019.pdf (Accessed 8 July 2025).
FATF (2024) FATF's assessment of the United States. www.fatf-gafi.org/en/countries/detail/United-States.html (Accessed 8 July 2025).
FATF (n.d.) FATF's assessment of Luxembourg. www.fatf-gafi.org/en/countries/detail/Luxembourg.html (Accessed 8 July 2025).
FATF-GAFI (2016) *Anti-money laundering and counter-terrorist financing measures – United States*, Fourth Round Mutual Evaluation Report, FATF, Paris (Accessed 8 July 2025).
FATF-GAFI (2022, April) Report on the State of Effectiveness and Compliance with the FATF Standards. www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness-compliance-standards.html (Accessed 8 July 2025).
FATF-GAFI (2023, February) 'Black and grey' lists. www.fatf-gafi.org/en/countries/black-and-grey-lists.html (Accessed 8 July 2025).
F AT F (2003) *Financial Action Task Force on Money Laundering. The Forty Recommendations.* www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202003.pdf (Accessed 8 July 2025).
FATF (2007) *FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing – High Level Principles and Procedures*, FATF. www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html (Accessed 8 July 2025).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

FATF (2013) *National Money Laundering and Terrorist Financing Risk Assessment*, FATF. www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf (Accessed 8 July 2025).

FATF (2022) *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations (2012 – Updated 2025)*, Paris. www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf (Accessed 8 July 2025).

Ferwerda, J. and Kleemans, E.R. (2019) Estimating money laundering risks: An application to business sectors in the Netherlands, *European Journal on Criminal Policy and Research*, 25(1), pp. 45-62 (Accessed 8 July 2025).

FinCEN (2024) *FinCEN Year in Review for FY 2023*, US Treasury. www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_508FINAL_2024_June_7.pdf (Accessed 8 July 2025).

García Fresno, M. (2022) *Analiza, que no es poco: Herramientas para el Análisis de Operaciones de Blanqueo de Capitales y de Financiación del Terrorismo*. Madrid: Fundación Notariado. https://publicaciones.notariado.org/p/-papel-analiza-que-no-es-poco-2 (Accessed 8 July 2025).

Grondona, V., Meinzer, M., Monkam, N., Schultz, A., & Villanueva, G. (2025) Which money to follow? Evaluating country-specific vulnerabilities to illicit financial flows. *European Journal on Criminal Policy and Research*, **31**, 667–693. doi:10.1007/s10610-024-09610-z (Accessed 8 July 2025).

Halliday, T. C., & Shaffer, G. (Eds.). (2015) *Transnational Legal Orders*, Cambridge: Cambridge University Press. doi:10.1017/CBO9781107707092 (8 July 2025).

Hopkins, M., & Shelton, N. (2019) Identifying money laundering risk in the United Kingdom: observations from national risk assessments and a proposed alternative methodology. *European Journal on Criminal Policy and Research*, **25**(1), 63–82.

Houston, J. F., Lin, C., & Ma, Y. (2012) Regulatory arbitrage and international bank flows. *The Journal of Finance*, **67**(5), 1845–1895.

ICIJ (2020, September 20) Explore the FinCEN Files data. www.icij.org/investigations/fincen-files/explore-the-fincen-files-data/ (Accessed 8 July 2025).

Jackson, G., Markevych, M., Bardin, Pierre, … Thomas, I. (2023) *Nordic-Baltic Regional Technical Assistance Report. Financial Flows Analysis, AML/CFT Supervision, and Financial Stability*, Washington, DC: International Monetary Fund (IMF). www.imf.org/-/media/Files/Publications/CR/2023/English/1EUREA2023003.ashx (Accessed 8 July 2025).

Janský, P., Meinzer, M., & Palanský, M. (2022) Is Panama really your tax haven? Secrecy jurisdictions and the countries they harm. *Regulation & Governance*, **16**(3), 673–704.

Jensen, R. I. T., & Iosifidis, A. (2023) Fighting money laundering with statistics and machine learning. *IEEE Access*, **11**, 8889–8903.

Lando, S., & Landry, M. (2023) The production and use of financial intelligence to counter terrorism and terrorist financing. In C. A. El Khoury, ed., *Countering the Financing of Terrorism*. International Monetary Fund. pp.63-88. www.elibrary.imf.org/display/book/9798400204654/CH003.xml (Accessed 8 July 2025).

Lannoo, K., & Parlour, R. (2021) *Anti-Money Laundering in the EU – CEPS*. Brussels: CEPS. www.ceps.eu/ceps-publications/anti-money-laundering-in-the-eu/ (Accessed 8 July 2025).

Lebid, O., & Veits, O. (2020) Search for statistically approved criteria for identifying money laundering risk. *Banks and Bank Systems*, **15**(4), 150–163.

Levi, M., Reuter, P., & Halliday, T. (2018) Can the AML system be evaluated without better data? *Crime, Law and Social Change*, **69**(2), 307–328.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Meinzer, M. (2016) Towards a common yardstick to identify tax havens and to facilitate reform. In T. Rixen & P. Dietsch, eds., *Global Tax Governance: What is Wrong with it, and How to Fix it*. Colchester: ECPR Press, pp. 255–288.

Meinzer, M., & Harari, M. (2023, June 13) Transforming our flagship indexes to be even more responsive and timely. https://taxjustice.net/2023/06/13/transforming-our-flagship-indexes-to-be-even-more-responsive-and-timely/ (Accessed 8 July 2025).

Meinzer, M., Harari, M., Lorenzo, F., & Knobel, A. (2023) Comparative report on SWIFT data in the EU27. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.4346192 (Accessed 8 July 2025).

Ministerio de Hacienda y Función Pública (2023) Orden HFP/115/2023, de 9 de febrero, por la que se determinan los países y territorios, así como los regímenes fiscales perjudiciales, que tienen la consideración de jurisdicciones no cooperativas, HFP/115/2023. www.boe.es/buscar/act.php?id=BOE-A-2023-3508 (Accessed 8 July 2025).

Nduka, B., Okenyebuno, E., & Sechap, G. (2021) Refocusing designated non-financial businesses and professions on the path of anti-money laundering and combating the financing of terrorism compliance. *Journal of Money Laundering Control*, **24**(4), 693–711.

Ogbeide, H., Thomson, M. E., Gonul, M. S., Onkal, D., Bhowmick, S., & Bello, A. U. (2024) Rethinking experts' perceptions in money laundering risk assessment. *European Journal on Criminal Policy and Research*, **31**, 753–777. doi:10.1007/s10610-024-09586-w (Accessed 8 July 2025).

Ogbeide, H., Thomson, M. E., Gonul, M. S., Pollock, A. C., Bhowmick, S., & Bello, A. U. (2023) The anti-money laundering risk assessment: A probabilistic approach. *Journal of Business Research*, **162**, 113820.

Omar, N., & Johari, Z. A. (2015) An international analysis of FATF recommendations and compliance by DNFBPS. *Procedia Economics and Finance*, **28**, 14–23.

Panevski, D., Peráček, T., Rentková, K. (2021) Analysis of the Practices of Financial Intelligence Units (FIUs) and Other Anti-money Laundering Agencies Within EU. In Kryvinska, N., Poniszewska-Marańda, A. (eds) *Developments in Information & Knowledge Management for Business Applications*. Studies in Systems, Decision and Control, vol 376. Springer, Cham.

Ping, H. (2005) The suspicious transactions reporting system. *Journal of Money Laundering Control*, 8(3), 252–259.

Reuter, P., & Riccardi, M. (2024) Introduction to special issue on 'understanding money laundering: empirical and theoretical insights into offenders, typologies, and determinants of criminal behaviour'. *European Journal on Criminal Policy and Research*, **30**(3), 327–332.

Riccardi, M., & Reuter, P. (2024) The varieties of money laundering and the determinants of offender choices. *European Journal on Criminal Policy and Research*, **30**(3), 333–358.

Richardson, B., Williams, D., & Mikkelsen, D. (2019) *Network analytics and the fight against money laundering*, McKinsey. www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering (Accessed 8 July 2025).

Ross, S., & Hannan, M. (2007) Money laundering regulation and risk-based decision-making. *Journal of Money Laundering Control*, **10**(1), 106–115.

Sachoulidou, A. (2023) Going beyond the 'common suspects': to be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. doi:10.1007/s10506-023-09347-w (Accessed 8 July 2025).

Sathye, M., & Islam, J. (2011) Adopting a risk-based approach to AMLCTF compliance: the Australian case. *Journal of Financial Crime*, **18**(2), 169–182.

Savona, E. U., Riccardi, M., Shelton, N., & Kleemans, E. R. (2017) Assessing the risk of money laundering in Europe: final report of project IARM. www.academia.edu/33455865/

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004

Assessing_the_Risk_of_Money_Laundering_in_Europe_Final_Report_of_Project_IARM (Accessed 8 July 2025).
Sciurba, M. (2018) The heart of know your customer requirements: the discriminatory effect of AML and CTF policies in times of counter-terrorism in the UK. *European Journal of Crime, Criminal Law and Criminal Justice*, **26**(3), 222–235.
Sharman, J. C. (2010) Dysfunctional policy transfer in national tax blacklists. *Governance*, **23** (4), 623–639.
Shiel, F., & Starkman, D. (2020, September 19) About the FinCEN Files investigation – ICIJ. *International Consortium of Investigative Journalists (ICIJ)*. www.icij.org/investigations/fincen-files/about-the-fincen-files-investigation/ (Accessed 8 July 2025).
Singh, K., & Best, P. (2019). Anti-money laundering: using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, **34**, 100418.
Takáts, E. (2007). *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement*. Washington, DC: International Monetary Fund. www.imf.org/-/media/Websites/IMF/imported-full-text-pdf/external/pubs/ft/wp/2007/_wp0781.ashx (Accessed 8 July 2025).
Tax Justice Network (2025, June 3) Financial Secrecy Index: The world's biggest enablers of financial secrecy. https://fsi.taxjustice.net/ (Accessed 9 September 2025).
Turksen, U., Benson, V., & Adamyk, B. (2024) Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI. *Journal of Banking Regulation*, **25**, 359–377. doi:10.1057/s41261-024-00233-2 (Accessed 8 July 2025).
Unger, B. (2023) *Reforming EU blacklisting: how to increase the effectiveness and avoid politicisation of the EU list of high-risk jurisdictions for anti-money laundering and counter-terrorism financing: US experience and considerations for EU reform*, European Parliament Committee on Economic and Monetary Affairs (ECON). www.europarl.europa.eu/RegData/etudes/STUD/2023/740091/IPOL_STU(2023)740091_EN.pdf (Accessed 8 July 2025).
United Nations (n.d.) goAML: Anti-Money Laundering System. https://unite.un.org/goaml/ (Accessed 8 July 2025).
US Congress (2024) United States Code, 2018 Edition, Supplement 5, Title 31 – MONEY AND FINANCE, 31 USC 310 (2024). www.govinfo.gov/app/details/USCODE-2023-title31/USCODE-2023-title31-subtitleI-chap3-subchapI-sec310 (Accessed 8 July 2025).
Vedrenne, G. (2023, November 22) STR volumes rise again in Europe, Finland notwithstanding. *ACAMS Moneylaundering.Com*. www.moneylaundering.com/news/str-volumes-rise-again-in-europe-finland-notwithstanding/ (Accessed 8 July 2025).
Xue, Y.-W., & Zhang, Y.-H. (2016) Research on money laundering risk assessment of customers: based on the empirical research of China. *Journal of Money Laundering Control*, **19**(3), 249–263.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 18 Nov 2026 at 00:52:17, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009623605.004