THE SIXTH BAHAMAS CONFERENCE ON FINANCIAL CRIME

The Central Bank
of the Bahamas

Inter-American
Development Bank

March 2025

The opinions expressed in this work are those of the authors and do not necessarily reflect the views of the Inter-American Development Bank, its Board of Directors, or the countries they represent.

THE SIXTH BAHAMAS CONFERENCE ON FINANCIAL CRIME

AUTHOR:

JASON SHARMAN

SUPERVISORS:

FRANCESCO DE SIMONE AND GUILLERMO LAGARDA

About **the Conference**

This learning material summarises the main findings of the papers presented at the Sixth Bahamas Research Conference on Financial Crime. The conference was once again hosted in a hybrid in person/online format by the Central Bank of the Bahamas 15-17 January 2025. This year the conference saw 112 participants registered to attend in person, and around 280 online. Reflecting a trend towards a greater public profile than in previous years, proceedings were recorded and are now available via YouTube. The conference was funded by a levy on the Bahamian financial sector, with supplementary support from the Inter-American Development Bank.

The conference benefited from the participation of officials from the Inter-American Development Bank, the International Monetary Fund, the Latin American and Caribbean regional Anti-Money Laundering (AML) bodies (CFATF and GAFILAT, and the Financial Action Task Force. Support generously provided by the Inter-American Development Bank enabled the attendance of officials from the Financial Intelligence Units of Belize and Trinidad and Tobago, as well as simultaneous Spanish translation. A range of senior representatives from the Bahamian regulatory sector were in attendance, and the conference was opened by the Governor of the Central Bank of The Bahamas, Mr John Rolle. The inclusion of the private sector was again an important asset in both formal presentations and informal feedback and discussion from the floor.

The conference retained largely the same format as in previous years, with two days of paper presentations complemented with two discussion sessions, preceded by a closed speakers' session on the evening of the 15th January.

Abstract

The Sixth Bahamas Conference on Financial Crime, co-hosted by the Central Bank of The Bahamas and the Inter-American Development Bank in January 2025, brought together over 390 participants—both in-person and online—including policymakers, regulators, academics, private sector professionals, and representatives from regional and international institutions. The conference featured research papers, grouped into five thematic blocks: the overall effectiveness of anti-money laundering (AML) frameworks; the role of big data and new technologies; applied insights from regulators and compliance professionals; the use and misuse of AML laws; and transnational patterns in financial crime and regulatory responses. The first theme explored the core question of whether AML systems have been effective after three decades of implementation, prompting critical reflection on performance measurement, unintended consequences, and reform prospects. The second block examined how big data, machine learning, and digital monitoring tools are being deployed—albeit unevenly—to detect financial crime and improve institutional responses. The third set of papers focused on practical regulatory strategies, highlighting the value of empirical, risk-based supervision and the need to reassess overly burdensome or ineffective compliance requirements. A fourth theme raised concern over the abuse of AML laws to target political opponents and restrict civil society, revealing troubling patterns across both authoritarian and democratic contexts. Finally, a fifth group of contributions addressed the international dimensions of financial crime—including illicit network mapping, the evolution of tax information exchange, and the regional impact of de-risking on small economies. The conference emphasized the challenges to close the distance between AML research and practice, the limitations of current enforcement models, and the urgent need for more targeted, evidence-driven, and context-sensitive approaches to financial crime prevention.

Key Words: Money Laundering, Financial Crime, FATF, AML, Effectiveness, Compliance

The Big Question: Is Anti-Money Laundering Effective?

The focus of the speakers' session immediately preceding the conference was a long, synoptic paper by **Nazzari** and Reuter asking perhaps the most important question in Anti-Money Laundering (AML): after 35 years, how effective is AML policy? This paper represents a landmark in the broader study of money laundering and AML. It is something of stock-taking update on Reuter's 2004 book (co-authored with Edwin Truman) *Chasing Dirty Money: The Fight Against Money Laundering*, something of a classic in the field. It also updates another definitive long paper from 2006 asking the same question authored by Reuter and Michael Levi (who also attended the conference). The presence of FATF Vice-President Jeremy Weil as an informal respondent to the paper was a great asset to the session, and indeed the conference more generally.

The tone of the paper might best be described as guarded pessimism. In blunt terms, the conclusion is that 'There is simply no evidence that money laundering is in decline or that it has become more difficult or expensive to launder criminal money.' This is undoubtedly a damning verdict, especially as the cost and intrusiveness of the global AML apparatus has continued to grow and grow. It is also important to note that this conclusion is hedged in a couple of important respects. First, the authors note that problems with the quantity and quality of evidence available mean that any verdict on AML effectiveness, positive or negative, can only be tentative. Second, it seems that AML policy may actually help fight other sorts of crime apart from money laundering, at least in the United States. Nevertheless, these caveats do not change the basic message of the paper: AML is an expensive failure. What is the basis of this pessimism?

Nazzari and Reuter suggest that most money laundering schemes are relatively simple and crude. Indeed, for most drug proceeds there may not be any need to launder within the formal financial system at all; dealers get paid in cash, and use this cash to pay for more illicit goods to sell, and then for everyday expenses. The fact that a large proportion of criminal money may not actually need to be laundered is a profound finding, striking as it does against a central presumption of the current AML edifice. At the other end of the scale, the huge fines routinely and repeatedly levied against major international banks show that they are unable or unwilling to stop the flow of dirty money passing through their accounts. The authors note that the AML system imposes high but unquantifiable costs, especially on developing countries, who are often coerced into implementing policies that have little relevance for their needs and circumstances. Accordingly, the paper calls for a deep re-think of AML policy, but the authors are again pessimistic about the prospects of meaningful reform.

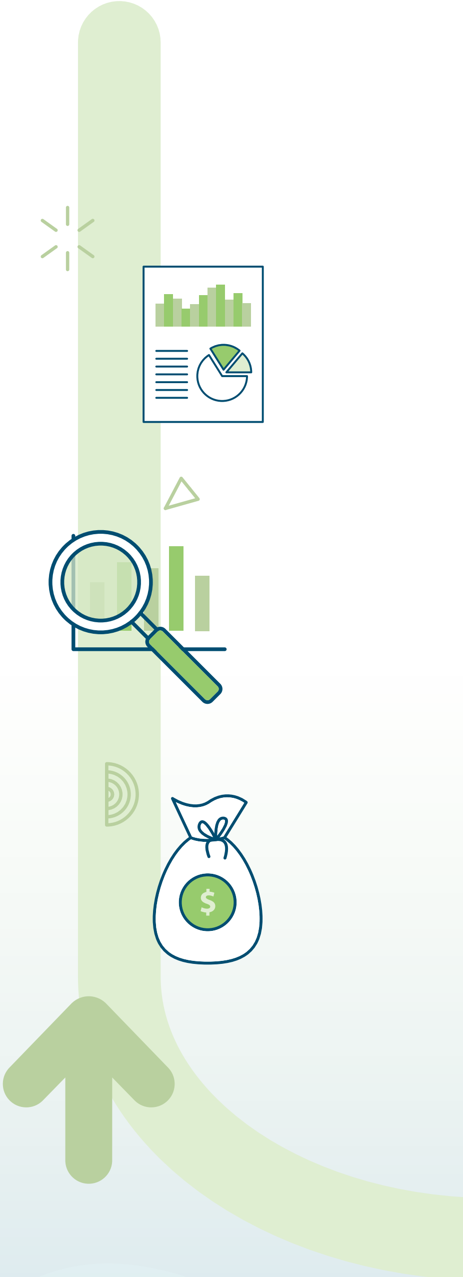
Not surprisingly, the FATF Vice-President contested this unflattering verdict of AML ineffectiveness. He argued that the AML system is a work in progress, and that the fifth round of mutual evaluations will have a re-doubled emphasis on effectiveness, as opposed to the focus on technical compliance in the first three rounds. Another objection raised to the paper was that lacking a counter-factual (what would the world be like without AML?) we simply cannot pass such a sweeping verdict on the system. This is a persistent challenge in evaluating public policy.

In some ways this contested first session crystalises the much more general tension between academics researching AML and policy practitioners. Speaking of the AML system, the former, like Nazzari and Reuter, are wont to say, ‘it's not working’; the implicit response from policy-makers is, ‘it's not changing’. Navigating this tension in a productive manner is perhaps the central ongoing challenge of the conference, and probably of any effort to bring academics and practitioners in dialogue on this topic.

Big Data and AML

The need for more (and better) data has been a recurring theme of the conference over the years, not only to get a sense of the AML system's effectiveness (or ineffectiveness, as the case may be), but also to identify where laundering and predicate crimes are occurring. Over the years the conference has seen considerable progress as researchers have shown great originality and creativity in responding to, if not definitively solving, this challenge.

In this spirit, the multi-authored paper presented by **Ferwerda** uses real (anonymised) transaction data from the Danish Spar Nord Bank to 'search for smurfs'. In money laundering parlance, smurfing refers to obscuring large flows of criminal money into a bank by breaking them up into many small, individually innocuous looking transactions. From the money launderer's point of view, the aim is to make each transaction small enough to slip below a bank's reporting threshold. But in order to do so, of course, criminals have to know what the threshold value is. Ferwerda and his co-authors sought to determine whether such smurfing was occurring in Spar Nord Bank by looking for suspicious clustering around certain amounts that are unlikely to have arisen by chance. For example, if the reporting threshold was 7,500, and there were a very large number of deposits at 7,499, this would indicate money laundering via smurfing. Previous papers at the conference have shown this suspicious transaction bunching or clustering of transaction values just below those that trigger reporting or regulatory requirements (e.g. Karen Nershi on crypto-currency trading). Happily the paper did not find evidence of smurfing. To their great credit, the authors will make their methodology for finding smurfs available free and online for any other bank or financial institution to use. This work is thus a clear demonstration of the practical value of academic research on AML.



A critique of Artificial Intelligence and associated technologies is that their impact is clear in stock market valuations, but invisible in productivity figures. Perhaps along the same lines, the application of similar technologies to AML might prompt an equivalent complaint in terms of a lack of discernible impact. The paper by **Siu and Hutchings**, a genuine big data study, may be a sign that this is changing. It investigates social media cryptocurrency frauds, a new and rapidly growing area of financial crime, given that there are now over 600 million cryptocurrency users. The authors use machine learning models to sift through 45.2 million posts relating to crypto investment on Bitcointalk, 2.3 million posts on Reddit, and 173,000 relevant YouTube videos. On the principle that if something looks too good to be true, it is, 94,821 scam advertisements are identified as those offering implausibly high returns over the very short term (e.g. doubling deposits in a few days or even hours). Tracing these adverts back leads to 1554 Bitcoin addresses, serving as a mix of 'decoys', designed to present an impression of substantive investment success, and deposit addresses used to accept transfers from scam victims. Though the paper eschews policy recommendations, it is remarkable the extent to which such crypto scams are hiding in plain sight, and the extent to which scammers can ply their trade unmolested by law enforcement, or social media companies.

Since its inception the conference has consistently benefited from a strong Italian contingent of presenters. The co-authored paper 'Mafias and Firms' presented by **Marchetti** continues this tradition, with authors from the Bank of Italy's Financial Intelligence Unit as well as academia. The Italian research strength in financial crime in large part reflects a close and productive partnership between policy-makers and academics, often reflected in extensive data sharing. The Marchetti paper is indicative of the rewards of such collaboration, which unfortunately is the exception rather than the rule beyond Italy.

Working from a unique confidential data-set of approximately 100,000 firms under suspicion of having ties to organised crime (the *Mappatura*), the authors find that criminals' links with business fall into three main categories, which co-vary with firm size. For smaller firms, the relationship between crime and business fits the conventional picture: mafiosi use small, usually cash intensive businesses to launder the proceeds of their crimes. When it comes to medium-sized firms, however, the strategy is likely to be different. Criminals enhance these firms' business prospects by using threats or bribes against competitors. The most novel finding, however, is that criminals' connections with large firms seem to reflect a desire to network with elites, rather than these connections being formed to directly advance criminal activity (e.g. money laundering). Aside from the considerable merits of the paper itself, it prompts the question of whether other countries' FIUs have an equivalent central data-base of criminally suspect firms, and if so whether researchers could make use of anonymised data.

A second paper working from Italian data by **Siino** and co-authors takes a similar big data approach to detecting corruption and organised crime risk in government procurement. The paper once again demonstrates how far ahead Italy is in the willingness of law enforcement and other government agencies to share confidential data in order to advance knowledge of financial crime.

The paper is based on 2.1 million government procurement contracts awarded 2018-2023, representing E2.8 billion of public money. Rather like Siu and Hutchings sifting of millions of social media ads, the Siino et al. paper look for 12 indicators of corruption risk, for example single-bidder tenders, or direct awards without any tendering process. A threat to inference is that over half of the recorded instances are missing data on the contracting process, and these missing data are not distributed randomly. Put differently, the missing data may be an indicator of corrupt conduct. The available data suggest that the North of Italy is more prone to procurement corruption than the South, but there is much more missing information on contracts from the South than the North, which may flip the picture. The findings are then matched against the same mappatura database of firms suspected to have links with organised crime as used in the Marchetti paper. Public procurement contracts involving these firms are 'more opaque, less competitive and more frequently entail the use of discretionary powers by the contracting authority'. Firms linked with organised crime are significantly more likely to score high on the composite of risk indicators than those without such links, tending to confirm the validity of this measure. More broadly, this study illustrates how anti-corruption agencies and Financial Intelligence Units can use big data to isolate risky transactions most in need of investigation.

Applied AML: **Law Enforcement, Regulatory and Compliance Industry Insights**

Speaking of AML researchers and practitioners might suggest that these are separate worlds, but the second group of papers at the conference was by those at the sharp end of the AML system, featuring contributions from law enforcement, regulators and the compliance industry.

Working in Britain's National Crime Agency (NCA), **Lawrence** presented an overview of changing patterns in criminal finance over the last decade. This perspective emphasised the importance of advancing technology in money laundering, especially the use of cryptocurrency, but also AI-enabled fraud. Organisationally, criminal finance is said to have become more international. At the same time, cash and traditional informal value transfer systems like hawala remain important. It is interesting to contrast this view with the Nazzari and Reuter paper already discussed, and with previous conference papers by Michele Riccardi and various co-authors. In contrast to the Lawrence paper, these suggest that money laundering is usually small-scale, low-tech, and local. Whether money laundering is changing (perhaps with the declining use of cash in Western Europe and North America), or whether money launderers are more advanced in the UK, or whether one of these contrasting perspectives is simply wrong, is hard to say.

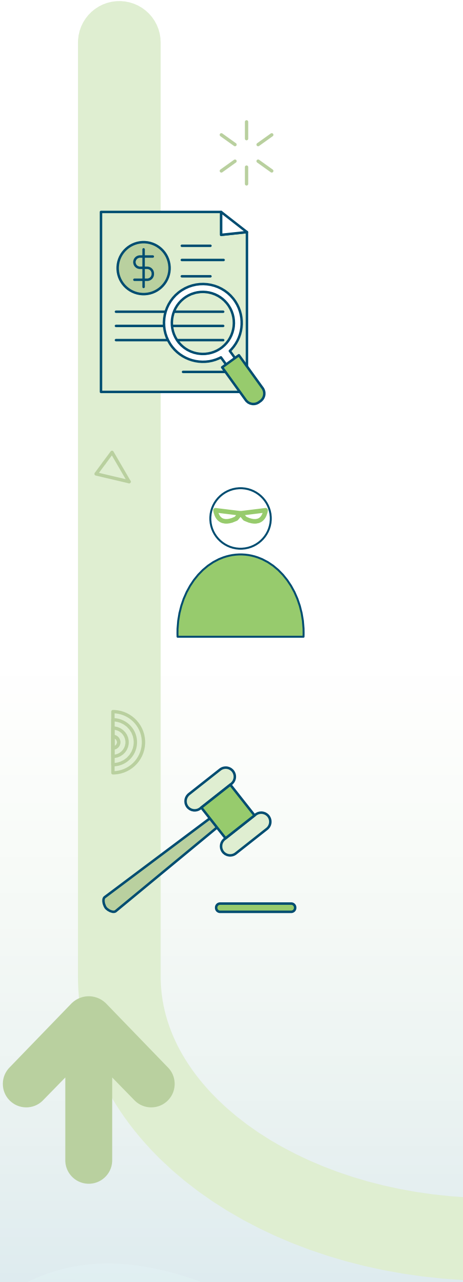
A joint paper from **Minus-Springer**, Adderly and Littrell (the former conference director) takes a practical look at how regulators can use existing data sources to improve their AML regulation. A recurrent problem in AML policy has been to identify areas of particularly high money laundering risk, something of a holy grail for the risk-based approach that is meant to be the guiding principle in the field. The logic is clear: regulators have limited time, attention and money, and thus these resources should be directed at areas of higher money laundering vulnerability, where they will result in the largest return. The consistent stumbling block, however, is the difficulty of accurately identifying these areas of greatest risk.

Proceeding by a basis of elimination, the paper performs a valuable practical service by eliminating sectors that are likely to present low money laundering risk. These low-risk sectors and channels include luxury cars, high denomination US dollar bills (around 80 per cent of the more than 2 trillion of US cash stock world-wide is 100 dollar bills), and the gaming sector. This process of eliminating low-risk sectors may well be a more solidly grounded path to a more risk-based approach to AML supervision than under- or unevidenced guesses about where money laundering occurs. In the Bahamian context this new approach to supervision had been delayed by the disruption of first Hurricane Dorian, and then the Covid pandemic, illustrating that, as with politics, AML policy is the art of the possible.

The paper from the private compliance industry by **Timm** drew on a very large ACAMS (the Association of Certified Anti-Money Laundering Specialists) consultation exercise including both surveys and face-to-face meetings. The paper included some important practical solutions to improve AML effectiveness. According to the thousands of ACAMS members surveyed, one of the most basic improvements would be for authorities to more precisely specify to regulated private sector firms the goals of AML policy. For example, catching money launderers and preserving the integrity of the financial system are different goals that often require different approaches, but both are elided under the label of AML. The implication that thousands of compliance industry specialists at present don't know what the AML system is designed to achieve, even when this system has been in place for over 30 years, is not reassuring.

A similarly practical suggestion would be for regulators to ask the banks and other firms they regulate which AML requirements are the most burdensome and least productive. Harking back to shortcomings in applying a risk-based approach, the ACAMS paper suggests that in practice banks and other reporting entities try to cover everything, rather than using intelligence to concentrate their scrutiny in particularly high-risk areas. Another valuable suggestion was that private sector AML officers be given much greater flexibility by regulatory supervisors to pursue a genuinely risk-based approach by changing the principle by which these officers are assessed. Once regulators assessed that a given AML program was properly resourced and the staff properly qualified, officers would be free to design their institution's AML program, unless supervisors could prove a specific abuse of discretion. Such an approach helps to combat the seemingly widespread problem of firms spending huge amounts of time and money on AML policy they know to be useless, but which they feel they have to perform to satisfy regulators. The problem of defensive reporting or junk reporting, i.e. flooding the system with a high volume of low-quality Suspicious Transaction Reports, might be an example of this more general AML pathology. In general the paper is a refreshing demonstration of how there are simple things that could (and should) be done to meaningfully improve AML effectiveness.

Use and Abuse of Anti-Money Laundering Laws



If there is one profession that dominates the commanding heights of global AML policy it is lawyers, rather than economists or criminologists. The first paper on AML law by Wegner focuses on Article 75 of the Sixth European Union Anti-Money Laundering Directive. This provision is designed to address what has been something of an Achilles heel of the AML system: the tendency of banks to work in isolation from each other in calculating risk and detecting suspicious transactions. Article 75 seeks to enable banks to share information on their customers so as to better fit together the pieces of the AML puzzle. Yet this laudable aim cuts against strong EU data protection provisions. At one level an attempt to reconcile these contradictory regulatory principles of information sharing and data protection, Wegner argues that Article 75 has instead merely reproduced this contradiction by trying to uphold both. It seems that banks will be left to work out this muddle for themselves, with the probable consequence that private sector risk aversion will mean that very little information is shared.

If so, this outcome is somewhat reminiscent of problems in FATF-mandated de-risking. Banks were told to be discerning in cutting ties with customers only on a risk-based basis, but also that they would face fines if they retained clients that were too risky. Banks tended to resolve this tension by erring on the side of caution, cutting whole classes of customers (e.g. money remitters) to reduce the chance of fines. If regulators are not clear on their priorities, throwing the problem to the private sector to work out is rarely a recipe for success.

Although the abuse of AML laws to persecute political opponents has been termed an ‘unintended consequence’ by the FATF, unlike the clash of principles above, all too often governments have been entirely calculating in using AML laws in this manner. **Reimer’s** paper is a much needed and long overdue study of how AML rules have been used by authoritarianand democratic governments alike to target political opponents.

The AML system has steadily weakened the presumption of innocence, most recently in mandating that countries should be able to confiscate people's assets without a conviction. Beyond this, the threshold for freezing assets is even lower, usually just reasonable suspicion. Reimer stresses that the problem is not just the controversial Recommendation 8, which regulates Non-Profit Organizations, but one that runs throughout the AML system. Thus even if governments are abiding by their own laws (and many of course do not), there is ample scope for them to use the AML system to pressure opponents. Dictatorial governments already have a wide range of tactics for targeting opponents, but AML laws give them a useful veneer of legality while doing so. But democratic governments from India to Canada have also succumbed to this temptation. In response, the FATF Vice-President stressed that curbing the political misuse of AML in the manner revealed by Reimer's paper is now a priority for the FATF.

Mapping Global and Regional Networks

There is something of a paradox in global AML policy: despite broad agreement that the problem is inherently transnational, much of the policy response is strictly national. Mutual Evaluation Reports look at one country at a time in isolation, and National Risk Assessments are exactly what they say they are. Even different branches of the same bank may have difficulty sharing information across borders. Each of the three papers below transcends these limits in different ways.

Haberly's paper reports on a huge global mapping project that provides a unique big picture sense of different kinds of illegal cross-border flows. Furthermore, it also tracks change over time in these flows and networks. One of the most important punchlines is foreshadowed in the title, 'From London to Dubai-Kong'. This formula functions as something of a short-hand to describe the displacement of the financial architecture of many illicit actors from the West, centred on London, to the 'post-Western' financial centres of Dubai and Hong Kong.

The data-set on which the paper is based maps several different kinds of networks. Illicit financing, what Haberly terms 'guerilla financial networks', is mapped by the nationality of approximately 10,000 entities (people and companies) appearing on US sanctions lists between 1980 and 2023. These sanctions lists have expanded enormously over time in number and scope as financial sanctions have become the transnational weapon of choice for the United States government. Most of the data is taken from the US Office of Foreign Asset Control, supplemented by commercial data-bases.

Contrary to stereotypes of footloose illicit money flitting from one jurisdiction to another, Haberly sees a great deal of inertia, of 'stickiness', whereby actors' finances are embedded in particular contexts. Relocations only occur as a result of sharp or sustained pressure. Mild pressure will mean that targeted networks persist in place; more severe pressure will mean relocation of the network from one major financial centre to another; the most severe pressure will produce dispersal to the margins of the global financial system. Haberly sees these three contrasting possible outcomes in foreign bribery networks, still centred on the West, Iranian and Russian sanctions-busting networks, relocated to Dubai and Hong Kong, and Islamic State financing, driven to Africa and the Indian Ocean. The data-set represents an incredibly valuable new resource for scholars and policy-makers alike. More generally, the project provides a signal lesson in using big data to help us to see the wood for the trees, rather than just exacerbating an already severe information overload.

Morriss and Ku's paper changes the focus from financial sanctions to tax, more particularly tax information exchange, but is equally concerned with change over time in global networks. Above all, the paper is styled as busting the myth of tax havens as 'sunny places for shady people', secrecy jurisdictions that thrive on foreign tax evasion money. Looking at global tax policy is an instructive counter-point to AML. Both areas have seen a vast expansion in the cross-border exchange of financial information since the late twentieth century (in 2022 tax information exchange involved 123 million bank accounts holding E12 trillion). Intriguingly, the impact of this information exchange seems to have been much more substantial in curbing tax evasion than in limiting money laundering, although as ever the standard caveat about the limits of the evidence once again applies. For their part, Morriss and Ku take an unequivocal line that old-fashioned international tax evasion is now dead.

For critics, the rationale for tax havens is obvious: they provide secrecy to hide dirty money, including that evading taxes. Now, however, all the world's financial centres (with one glaring exception) automatically exchange tax information through the OECD Common Reporting Standard. Yet most offshore centres are still in business, and indeed the most important ones are thriving. How can this be? Morriss and Ku trace the evolution of this global transparency regime, and the manner in which offshore centres have adapted.

The first efforts in this direction were purely bilateral arrangements centred on OECD countries which allowed for information exchange only within narrowly defined limits. Especially over the last decade or two, not only has the state-to-state network grown far more dense, but the painstaking and time-consuming mechanism of information exchange on request has been replaced by bulk automatic exchange. Within offshore centres, this transparency shift has necessitated fundamental regulatory change. In particular, they have set up independent regulators and licencing regimes for their Corporate Service Providers, often doing so ahead of their onshore peers.

Staying with the 'behind the border' effects of the multilateral regulatory initiatives, **Griffin** takes a Caribbean perspective on changes in the regional banking industry. At the broadest level, the paper sees small Caribbean states as being on the receiving end of often politicized and discriminatory rules and black-listing processes. The paper makes the point, confirmed by previous presentations at the conference from the International Monetary Fund, that bodies such as the FATF and European Union consistently over-diagnose financial crime risks in small, non-member jurisdictions and just as consistently under-diagnose such risks among their own members' much larger economies. Caribbean countries are shown to have a strong record of technical compliance with FATF standards, but nevertheless be disproportionately included on the various negative lists.

The last couple of decades have seen a withdrawal of many international (particularly Canadian) banks from the Eastern Caribbean states. Though the paper attributes this to AML-induced de-risking, in previous years other conference attendees have taken issue with this thesis, arguing that this retrenchment is a simple reflection of commercial rather than regulatory factors. Regardless of the cause, threats to correspondent banking ties are of very serious concern to these small, open economies, as much for reasons of trade, tourism and remittances as anything to do with international financial services. The upshot for the Eastern Caribbean countries might be a dilemma whereby they are 'too small to succeed', which a combined population of only 630,000, while also being stuck with a regional bank that is 'too big to fail'. This is the Trinidadian Republic Bank, which has largely stepped into the breach created by the withdrawal of other institutions.

Private Sector Perspectives

A basic goal of the conference from the beginning has been to bring together representatives from different communities with a common interest in financial crime, but which seldom interact with each other. In addition to researchers and policy-makers, the other key constituency is the private sector. As the Nazzari and Reuter paper makes clear, financial crime and AML more particularly are the most important example of governments delegating law enforcement responsibilities to the private sector.

Using anonymized data from Wells Fargo Bank, **Mold's** paper investigates fraud networks through tracing wire transfers. Fraud is perhaps the fastest growing area of financial crime, and as such increasingly central to money laundering. Whereas the laundering of drug proceeds may often take place in cash, income from fraud is much more likely to originate and remain within the banking system. In some ways akin to Siu and Hutchings' paper, Mold's analysis is focused on the sub-set of fraud-related transactions. These are 15,079 wire transfers involving a total of $767 million in 26 months 2021-2024. Fraud wires were transfers unauthorised by the originator, while scam wires were those where goods or services were paid for but not supplied.

Analysing these fraud and scam wire transfers revealed a number of commonly recurring attributes that help to identify risk. For example, it was common for criminals to send a low-value innocuous 'test' wire before making the larger illegal transfers. Transfers were often sent in bursts, with sums dispersed among beneficiaries only to be quickly re-aggregated further along the chain. Among recipients recently formed shell companies, or companies that had been struck off or dissolved were common. Certain 'regional corridors' repeatedly linked the same origin and destination countries for international fraud and scam transfers. Yet in some ways the very number and variety of potential risk factors in this area reproduces the basic needle-in-the-haystack problem of AML, that of isolating the small proportion of criminal transactions among the much larger number of legitimate ones.

The paper by **Ash** looks at the potential for financial institutions to use to AI and advanced data analytics to detect financial crime. The initial assumptions of the paper, that financial crime poses a threat to the stability of the overall financial system, and that financial criminals employ sophisticated and rapidly-evolving techniques, once again directly contradict the work of criminologists like Peter Reuter, Michael Levi and Michele Riccardi. Given this disagreement, claims like these must be evidenced rather than just asserted. Ash sees four main areas of opportunity for the application of new technologies. These are predictive analysis, network analysis, real-time monitoring and natural language processing applied to unstructured text. There are notable overlaps in the natural language processing model and that applied in Siu and Hutchings' research to detect social media adverts. Indeed, it would be impossible to carry out this sort of massive exercise without recent computational increases. So too there are overlaps in the network analysis suggested here and that demonstrated in practice by Mold with Wells Fargo wire transfers. Ash's paper illustrates the potential of some of these technologies with reference to Canadian insurance fraud.

Garcia and Namaat are similarly concerned with illustrating the potential of real-time transaction monitoring in the area of sanctions compliance for cross-border wire transfers. At present financial institutions using post-transaction monitoring may face a problem equivalent to locking the barn door after the horse has bolted, i.e. detecting non-compliant transactions after they have been posted. Compared to the consumer credit card data analysis used to pre-emptively block attempted fraud, analysis of international wire transfers is more sparse. Beyond this is the problem of a massive number of false positives flagged, a consistent problem in AML and sanctions screening that has only grown with the passing of time. A screening transformer model is said to provide an answer to this related set of problems. Transformer models were originally developed for natural language processing machine learning of the sort used by Siu and Hutchings, and referenced by Ash above. The goal here is to use the model to detect anomalous transactions and reduce false positives.

Positive initial results notwithstanding, there are challenges to be overcome. The paper notes that large institutions often face organizational barriers to the adoption of new technology, while smaller, more flexible organization may lack the data to make best use of the product. Banks and regulators arguably have a conservative risk-averse compliance culture (cf. the paper by Timm) that discourages new approaches. Data protection can be an obstacle, especially in Europe (see Wegner). Beyond the factors mentioned in the paper, the model includes risk factors such as jurisdictions being listed by the FATF or being a tax haven. Yet many papers previously presented at the conference have convincingly argued that whether or not countries are adjudged as tax havens or end up on one of the multilateral lists is as much a product of politics as any objective risk. For example, the IMF has pointed out that all of the countries listed by the FATF combined account for less than one percent of total international transfers. Finally and perhaps most fundamentally, reducing false positives depends on the ability to consistently identify the real positives, which of course is the very problem the AML system has been unable to solve.

In the end, the nagging doubt remains that for all the excitement (hype?) about Artificial Intelligence, big data, machine learning, and related advances, so far the application of all this new technology has made no discernable difference in the fight against money laundering and other kinds of financial crime.

Conclusions

In considering themes that reach across the papers presented at the conference it is helpful to return to the Nazzari and Reuter paper which seeks to provide a stock-take synopsis of our knowledge of money laundering and AML. If the paper is down-beat on progress in the practice of AML, what about in the study of AML? While it would be over-reaching to say that there are things we definitely know to be wrong or right, the range of uncertainty has narrowed.

For example, despite repeated claims from governments, the FATF and other international organizations, there is little evidence that money laundering or financial crime more generally threatens the integrity or stability of the overall financial system. More broadly, most outside observers and even the FATF itself in its 2022 stock-take paper judge the effectiveness of the current AML system to be low. There is general agreement that fraud and especially online fraud is a major growth area for criminals.

There are also matters of enduring disagreement at the conference over the years. Perhaps the most important of these is the degree to which money launderers use sophisticated and rapidly evolving schemes, or whether money laundering is generally crude, simple and local. So far the weight of evidence supports the latter view, but it is possible this may change over time, or vary with the type of predicate offence (e.g. online fraud vs drug dealing). A recurring difference concerns whether the various FATF and other lists can be taken as valid measures of jurisdictional risk, or whether they are reflections of power politics.

List of Conference Papers by Presenting Author

Ash, Gillian. "Leveraging Data Analytics for Enhanced Financial Crime Detection."

Ferwarda, Joras, Rasmus Ingermann Tuffveson Jensen and Christian Remi Wewer. "Searching for Smurfs: Testing if Money Launderers Know Alert Thresholds."

Garcia, Filipe and Ariel Naamat, "Beyond Sanction Screening: Leveraging Transformers for Comprehensive Real-Time Transaction Monitoring."

Griffin, Clifford. "The Complex World of Anti-Financial Crime Policies in the Caribbean."

Haberly, Daniel. "From London to Dubai-Kong: Mapping Geographic Shifts in US Sanctioned Global Financial Networks, 1980-2023."

Lawrence, Hilary. "The Evolving Nature of Illicit Finance–10 Years of Change."

Marchetti, Domenico J., Jaime Arellano-Bover, Marco De Simoni, Luigi Guiso, Rocco Machiavello and Mounu Prem "Mafias and Firms."

Minus-Springer, Duranda, Bonnielyn Adderly and Charles Littrell. "Deploying Empirical Analysis to Improve AML Supervision: A Bahamian Case Study."

Mold, Julia. "Analysis and Identification of Fraud and Money Laundering Networks."

Morriss, Andrew P. and Charlotte Ku, "The Evolution of the Global Tax Information Exchange Network."

Reimer, Stephen. "Weaponisation of the FATF Standards: A Guide for Global Civil Society."

Reuter, Peter and Mirko Nazzari. "How Well does the Money Laundering Control System Work?"

Siino, Marianna, Mario Gara and Stefano Iezzi. "Corruption Risk Indicators in Public Procurement: A Proposal Using Italian Open Data."

Siu, Gilberto Atondo and Alice Hutchings "A Study of Cryptocurreny Investment Scam Advertisements across Online Platforms."

Timm, Craig. "Incentivizing Effectiveness: Strategies to Achieve Better Anti-Financial Crime Results."

Wegner, Kilian. "Enhancing AML/CTF through Private Sector Data Exchange: What Opportunities does Article 75 of the New EU Money Laundering Regulation Offer for Collaborate Transaction Monitoring?"

THE SIXTH BAHAMAS CONFERENCE ON FINANCIAL CRIME

The Central Bank
of the Bahamas

Inter-American
Development Bank

March 2025