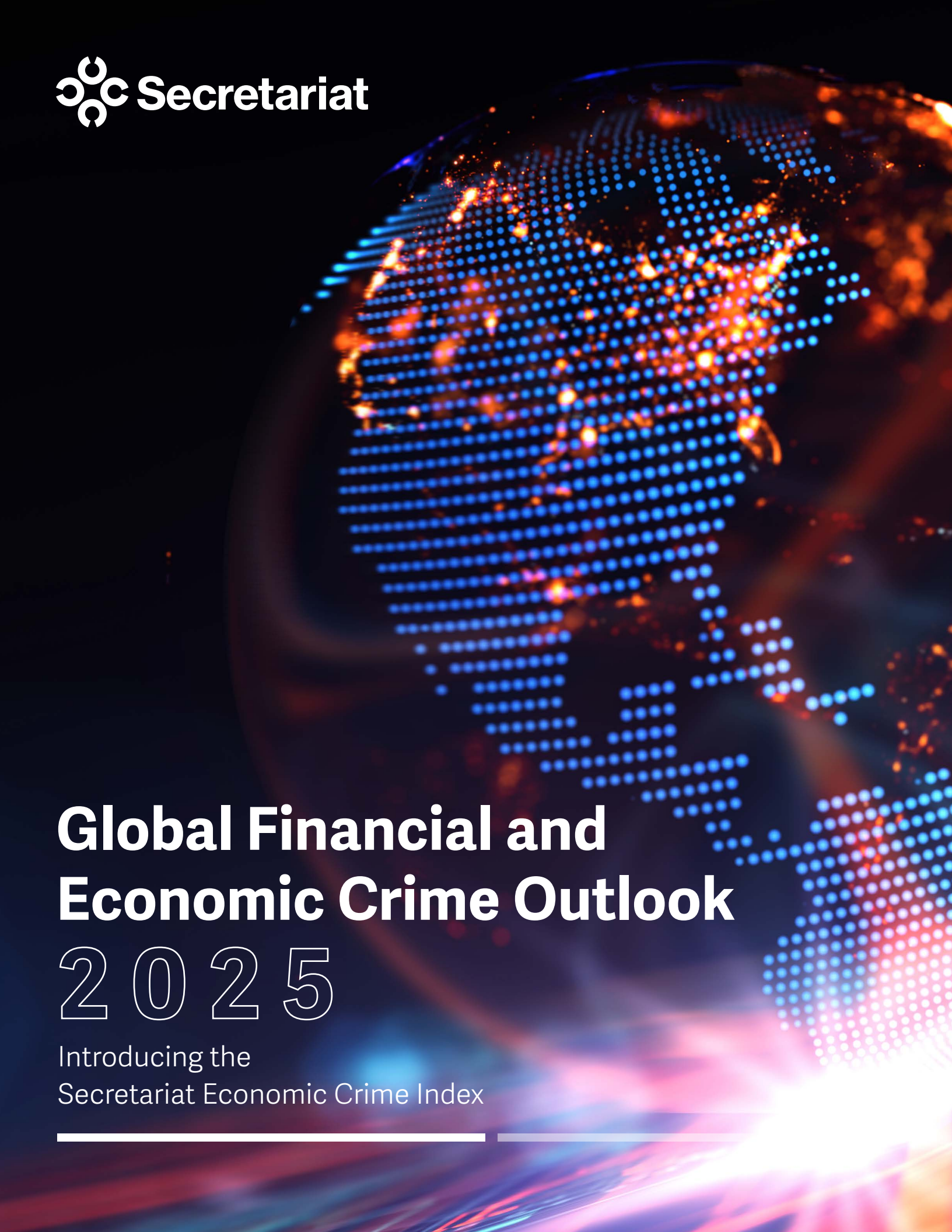
Secretariat



Global Financial and Economic Crime Outlook 2025

Introducing the
Secretariat Economic Crime Index

TABLE OF CONTENTS

FOREWORD

Mapping the Real Threats of Financial and Economic Crime in 2025

As risk professionals, we understand the global financial system's persistent and evolving threats. Financial and economic crimes — money laundering, terrorist financing, sanctions breaches, bribery, fraud, and market abuse — continue to strain our defenses. Compounding this challenge, the rapid evolution of virtual assets, decentralized finance (DeFi), artificial intelligence (AI), and machine learning presents new criminal methodologies and advanced detection tools.

The sheer scale of this threat, as highlighted by the International Monetary Fund (IMF) estimate of USD 800 billion to USD 2 trillion in annual money laundering, demands our attention. Secretariat estimates that these illicit flows could surge between USD 4.5 trillion to USD 6 trillion by 2030, underscoring the imperative for robust, data-driven risk assessments.

To address this critical need, my team and I at Secretariat have developed the *Global Financial and Economic Crime Outlook 2025*. Our inaugural annual report is designed to serve as your comprehensive guide to the global financial and economic crime landscape. We aim to empower you, our clients, with the insights necessary to make informed decisions, mitigate risks, and safeguard your interests.

This year's report comes at a time of significant regulatory flux. Rising economic protectionism, including the resurgence of tariffs and shifting geopolitical priorities, is reshaping enforcement agendas in key jurisdictions. While its long-term effects remain uncertain, the move reflects a broader trend of enforcement recalibration. These developments underscore the importance of proactive and globally attuned risk assessment. In today's volatile markets, basic risk checks are insufficient. You require a clear, objective understanding of potential threats. Our report delivers precisely that, providing an in-depth financial and economic crime risk evaluation. The Secretariat Economic Crime Index (SECI) is at the core of our analysis. This unique measure, ranging from 0 to 4, synthesizes data from critical areas: money laundering, corruption, and organized crime. By leveraging established indices like the Organized Crime Index, the Corruption Perception Index, and the Basel AML Index, the SECI transforms disparate data into a unified, actionable risk profile.

The SECI evaluates business viability in specific countries, setting a new standard for country risk assessment. We move beyond simplistic figures to comprehensively understand the multifaceted costs of financial and economic crime, including fraud, money laundering, corruption, and organized crimes.

Traditional risk assessments often fall short, relying on fragmented data and subjective opinions. Our report changes this narrative by providing a detailed, country-by-country index and rating, highlighting the strengths and vulnerabilities of 177 nations, and classifying these nations into four categories: Transparent Titans, Vigilant Players, Reactive Reformers, and Regulatory Laggards. We identify outliers, explain emerging trends, and provide the contextual understanding necessary for informed decision making, effectively mapping the complex pathways of financial and economic crime.

Furthermore, we look to the future. Drawing on our extensive experience, we identify the key financial and economic crime trends shaping the next decade. These insights offer you a strategic advantage in a rapidly evolving world. Proactive risk management is essential, and we are committed to equipping you with the knowledge to anticipate and mitigate future threats.

Whether you require country-specific data or insights into emerging trends, our report delivers critical information swiftly and effectively. We recognize the value of your time and have designed this report to be your essential financial and economic crime risk assessment resource.

Secretariat is committed to leading this critical discussion and serving as your vital partner in navigating the global financial arena. We are dedicated to fostering a safer, more transparent global economy, empowering you to make informed decisions, and safeguarding your interests.

Bhavin Shah, *Managing Director*
bshah@secretariat-intl.com

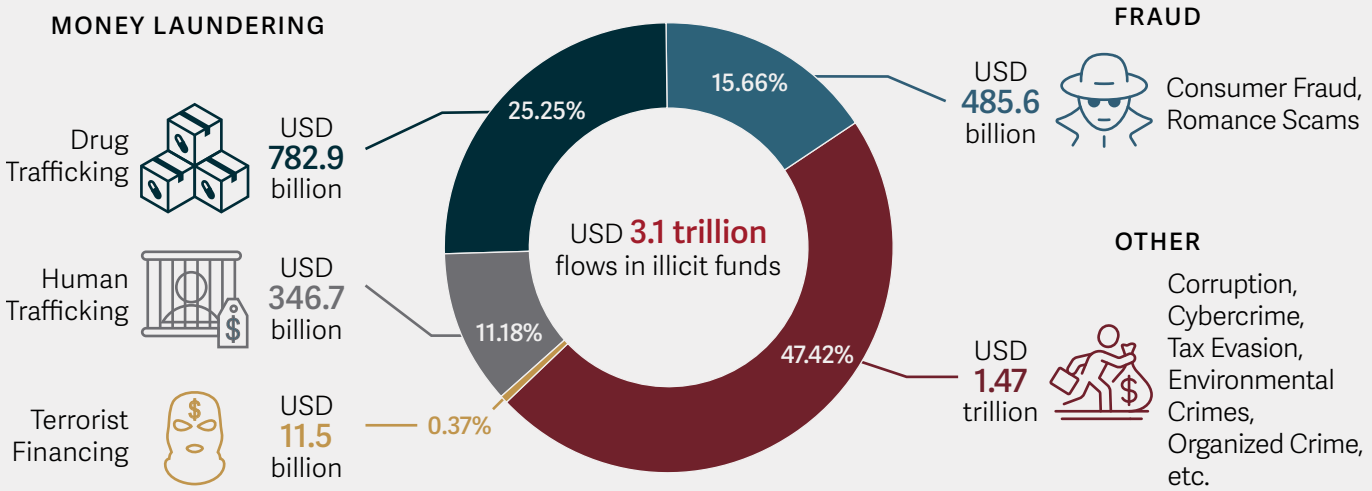
The Global State of Financial and Economic Crime

The global financial system faces a continuing threat from financial and economic crimes, such as money laundering, terrorist financing, breaches of economic sanctions, bribery, corruption, fraud, and market abuse. Looking at 2025 and beyond, this threat is set to intensify due to rapid technological advancements. Virtual assets, DeFi, AI, and machine learning are fundamentally changing both the methods used to perpetrate these crimes and the tools available to counter them.

This growing challenge is underscored by alarming statistics. The International Monetary Fund (IMF) estimates that "2% to 5% of global GDP" is laundered annually. Additionally, Nasdaq's 2024 Global Financial Crime Report reveals that approximately USD 3.1 trillion in illicit funds circulated within the global financial system in 2023. Most concerningly, the World Economic Forum's Global Coalition to Fight Financial Crime reports that law enforcement agencies seize or freeze less than 1% of these illicit proceeds.

The global landscape of anti-corruption enforcement is undergoing a notable transformation, partly driven by recent developments in the United States of America (US). On 10 February 2025, an Executive Order issued by President Trump introduced a temporary 180-day pause on enforcement of the Foreign Corrupt Practices Act (FCPA), alongside a stated shift in enforcement priorities. While

Breakdown of Global Illicit Financial Flows



Source: Nasdaq's 2024 Global Financial Crime Report

the longer-term implications remain uncertain, this may signal a recalibration of US engagement in international anti-bribery efforts.

Concurrently, governments are increasingly focused on domestic economic resilience, introducing protectionist measures such as tariffs and reassessing enforcement agendas. As a result, long-standing global norms around transparency and anti-corruption are being tested. In this evolving regulatory environment, concerns are emerging that certain financial crime risks — such as sanctions evasion, trade-based money laundering, and illicit capital flows — could become more difficult to detect and address, particularly where oversight is weakened or inconsistently applied.

This shift, unfolding against a broader backdrop of rising global financial crime, may create a temporary gap in international anti-corruption efforts. Companies operating in high-risk markets could perceive a reduced threat of US enforcement, which in turn may alter compliance behavior. In response, other jurisdictions, such as the United Kingdom and France, may strengthen their own anti-bribery enforcement, potentially contributing to a more fragmented and regionally driven global enforcement landscape.

These developments underscore the importance of agile, cross-border strategies to uphold financial integrity amid a shifting geopolitical and regulatory order.

Assessing Financial Crime: A Global Analysis of AML and Corruption

To minimize and mitigate financial crime risks effectively, a thorough assessment of jurisdictional vulnerabilities is essential, given the scale and complexity of these crimes. While financial crimes are inherently cross-border, certain regions are disproportionately susceptible due to weaknesses in regulatory frameworks, insufficient enforcement, and pervasive corruption.

Globally recognized indices provide valuable insights into these vulnerabilities, highlighting deficiencies in both the enforcement of Anti-Money Laundering (AML) compliance and governance structures intended to combat financial crime.

Our analysis focuses on two key risk factors that significantly influence the prevalence and frequency of financial crimes: money laundering and corruption. To better understand the interplay between these dimensions, we performed a comparative analysis across 177 countries. This involved plotting each country’s AML risk against its corresponding corruption risk, allowing for a clear visual representation of their relationship.

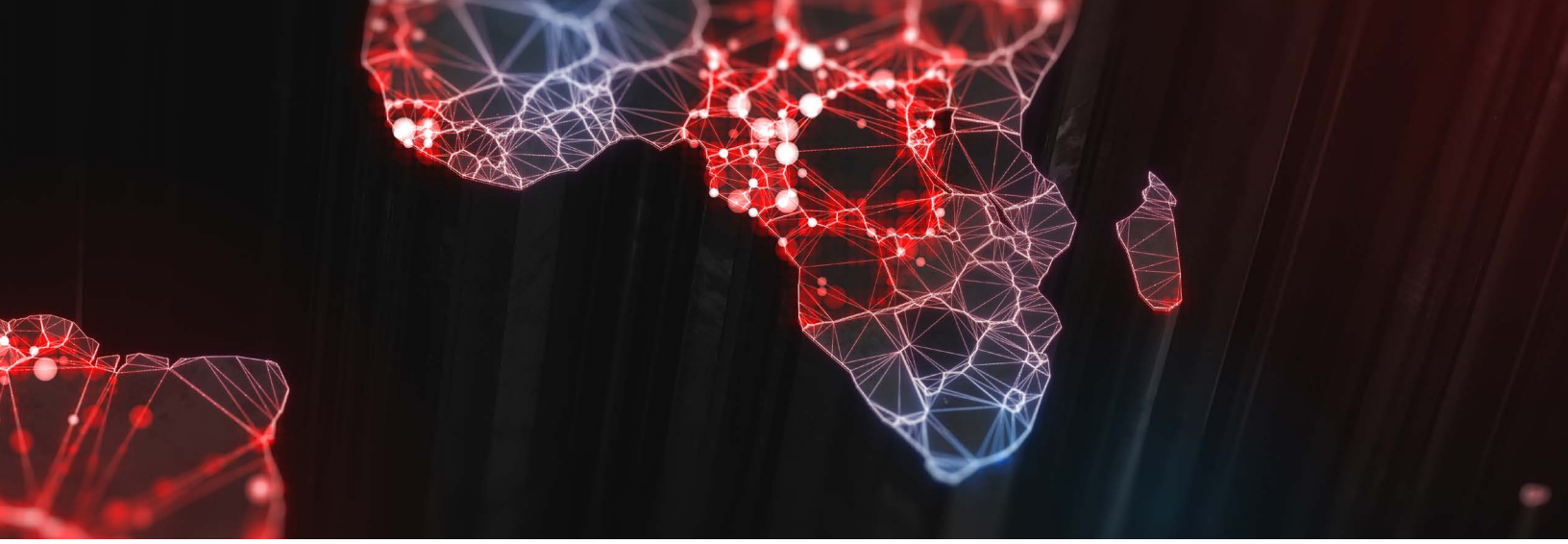
Mapping Global Risks: A Comparative Analysis

To visualize the interplay between money laundering risk and corruption risk, Secretariat constructed a scatterplot that categorizes economies into four distinct quadrants, each representing different levels of money laundering and corruption risks:

- The X-axis represents the money laundering risk scores.
- The Y-axis represents the scores that reflect corruption levels for a country.

Money Laundering and Corruption: A Comparative Risk Assessment Across Key Countries

Sources: The Basel AML Index and Transparency International's Corruption Perception Index



The global mapping of AML and corruption risks reveals distinct clustering patterns, with the majority of countries falling within predicted ranges. However, a few significant outliers highlight a divergence in how AML deficiencies and corruption risks align.

Some international financial hubs share an interesting commonality: Despite low corruption risk scores, they show comparatively high levels of money laundering risk. Low corruption does not eliminate financial crime vulnerabilities, particularly in jurisdictions that serve as key financial gateways with extensive banking and corporate services.

- **Switzerland and Luxembourg**: As major private banking hubs, these jurisdictions not only attract substantial legitimate wealth but also face risks from illicit funds seeking anonymity and asset protection. Despite strong legal and regulatory frameworks, their offshore banking services and wealth management sectors make them vulnerable to financial crime, particularly in the realm of private banking and investment funds.
- **Hong Kong and Singapore:** As global financial centers with extensive cross-border transactions, Hong Kong and Singapore appear to be prime targets for money laundering networks. While both benefit from strong oversight and low corruption, their financial complexity provides opportunities for illicit actors. Hong Kong has seen laundering schemes linked to mainland Chinese networks, while Singapore faces similar risks due to its role as a regional trade and finance hub. Unlike Switzerland and Luxembourg, where risks are concentrated in private banking, vulnerabilities in Hong Kong and Singapore often stem from trade-based money laundering, underground banking, and high-risk foreign inflows.
- **United Arab Emirates:** The UAE is the leading Middle Eastern financial center, actively improving AML compliance but historically facing scrutiny over free zones, high-value real estate transactions, and corporate opacity.

On the other hand, some countries reflect the opposite pattern — relatively strong AML frameworks but persistent high corruption levels, suggesting that systemic governance issues continue to undermine financial crime enforcement:

- **Russia:** AML controls exist, but widespread state-linked corruption skews enforcement. The ongoing conflict in Ukraine has led to increased international sanctions against Russia, further complicating its financial crime landscape.
- **Syrian Arab Republic:** Despite formal AML frameworks, the prolonged conflict and international sanctions have significantly weakened enforcement. Corruption within government institutions and illicit financial flows linked to war economies continue to pose significant financial crime risks.
- **Bangladesh:** While Bangladesh has strengthened AML regulations, enforcement remains inconsistent due to high levels of corruption, particularly in public procurement and banking. The Financial Action Task Force (FATF) has repeatedly highlighted deficiencies in risk-based supervision and financial transparency.

Introduction to the SECI: Our Approach to Financial and Economic Crime Risk Measurement

Existing indices, such as the Basel AML Index and the Corruption Perception Index (CPI), provide valuable insights into financial crime risks. However, while the CPI focuses exclusively on corruption perceptions, the Basel AML Index, though incorporating multiple data sources, places significant weight on FATF Mutual Evaluation Reports, which can be outdated for smaller jurisdictions. Recognizing the need for a more comprehensive measure, Secretariat developed the Secretariat Economic Crime Index (SECI): a proprietary country-level risk rating system assessing economic crime threats across 177 countries.

The SECI is a composite index, ranging from 0 (minimal risk) to 4 (maximum risk), that integrates three crucial dimensions of economic crime: organized crime, corruption and money laundering. It is constructed using a weighted average of data from three established global benchmarks: the Organized Crime Index, the Corruption Perception Index, and the Basel AML Index, with data statistically scaled for consistency before integration. It is important to note that while SECI does not feature a standalone fraud metric, it incorporates fraud-related risks through these existing indices. These indices capture elements such as bribery, financial misconduct, illicit financial flows, criminal enterprise, and fraudulent activities embedded within broader economic crimes.

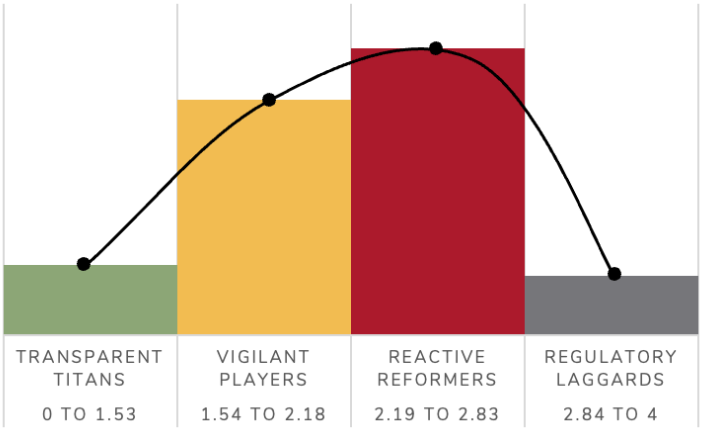
Evaluating Global Risk Disparities with SECI

To assess global risk disparities, we ranked 177 countries according to their SECI scores. These countries are then categorized into four tiers, reflecting their levels of transparency, the effectiveness of their anti-crime frameworks, and their overall exposure to economic crime.

- **Transparent Titans: 19 countries**, with SECI scores ranging from 0 to 1.53. These nations demonstrate transparency, robust anti-financial crime frameworks, and strong enforcement mechanisms, positioning them as leaders in preventing financial crime. While governance typically lowers economic crime risks, some financial hubs face unique vulnerabilities due to their vast financial sectors and cross-border activity. Yet, many remain Transparent Titans through proactive regulation and enforcement.
- **Vigilant Players: 64 countries**, with SECI scores between 1.54 and 2.18. The countries actively implement and evolve measures to address financial crimes and improve regulatory frameworks, proactively strengthening their systems against emerging risks. Some renowned financial hubs fall into this category, as their high exposure to financial crime risks necessitates constant regulatory evolution.
- **Reactive Reformers: 78 countries**, with SECI scores between 2.19 and 2.83. These nations exhibit weak anti-crime frameworks, significant regulatory gaps, and a higher prevalence of high-risk activities, facing challenges in effectively combating financial crimes due to insufficient regulatory measures.
- **Regulatory Laggards: 16 countries**, with SECI scores between 2.84 and 4.00. These nations are characterized by the dominance of illicit financial flows, deeply ingrained corruption, and systemic economic crime, rendering them vulnerable to widespread financial crime that often forms a core part of their functioning.

SECI Score Classification: Understanding Risk Tiers

Distribution of SECI Scores



The Distribution of SECI score chart displays the classification of 177 countries based on their SECI scores. The distribution follows a negatively skewed bell curve, meaning the curve is skewed to the left, with a longer tail on the lower (better-performing) end of the spectrum and a peak skewed toward the higher-risk categories. This implies that while a small group of countries performs exceptionally well in combating economic crime, the majority of countries cluster around moderate to higher-risk levels.

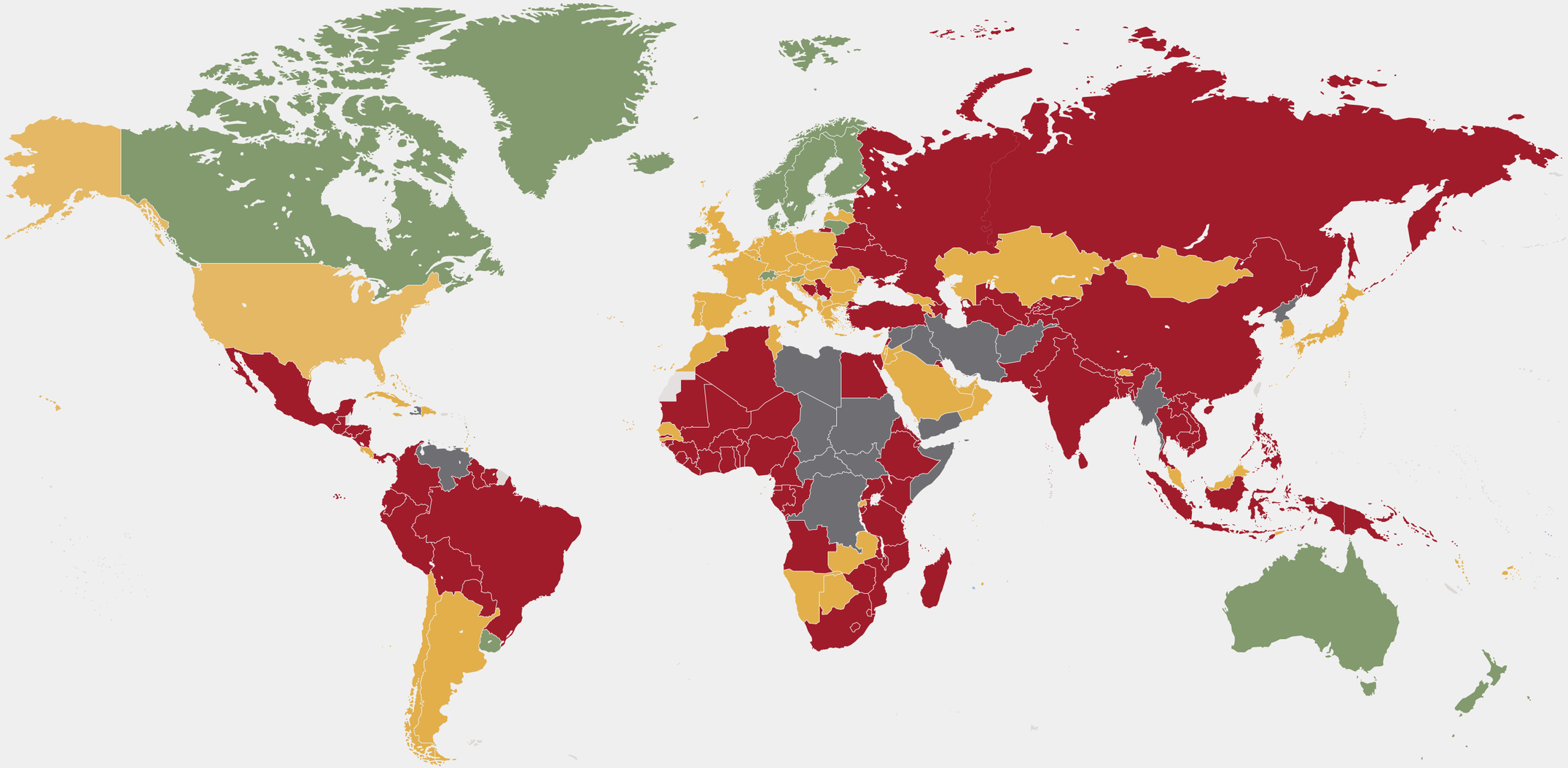
The classification is divided into four objectively derived tiers — Transparent Titans, Vigilant Players, Reactive Reformers, and Regulatory Laggards — based on statistically calculated thresholds from the mean.

The skewed distribution reflects the reality that economic crime risk remains a persistent and widespread challenge, with relatively few countries reaching high levels of transparency and control. Transparent Titans can serve as models for best practices and aid countries in lower tiers. Vigilant Players should continue to strengthen their systems and collaborate with other nations to share knowledge and resources. Reactive Reformers require significant investment in strengthening their legal and regulatory frameworks, as well as enhancing their enforcement capabilities. Regulatory Laggards necessitate comprehensive interventions, including international cooperation, to address systemic corruption and dismantle illicit financial networks.

In today's increasingly multipolar world, marked by rising geopolitical tensions and fragmented regulatory approaches, the fight against economic crime faces new and complex challenges.

The SECI distribution, skewed toward higher-risk jurisdictions, highlights the need for a collective progress. While nations understandably prioritize domestic interests in the wake of sanctions, tariffs, and shifting alliances, financial crime remains a transnational threat that no country can combat alone. The imperative now is to shift the peak of this curve to the left, toward stronger governance, enhanced enforcement, and cross-border collaboration. Moving the global center of gravity away from reactive reform and toward proactive transparency is necessary for economic resilience and long-term stability.

Secretariat Economic Crime Index



19 Transparent Titans

- Strong enforcement and global compliance
- High transparency and financial integrity
- Robust due diligence and reporting
- Proactive in tackling cross-border risks

64 Vigilant Players

- Evolving regulations and compliance
- Moderate financial crime exposure
- Active in global AML/CFT efforts
- Enforcement exists but with gaps

78 Reactive Reformers

- Weak enforcement and oversight
- Inconsistent regulatory frameworks
- Limited financial transparency
- Outdated AML measures

16 Regulatory Laggards

- High corruption and illicit flows
- Corruption entrenched in governance
- Systemic law enforcement and regulatory failures
- Minimal global cooperation

Transparent Titans

Rank	Country	SECI Score
1	Finland	1.01
2	Denmark	1.15
3	Iceland	1.16
4	Luxembourg	1.27
5	Estonia	1.27
6	New Zealand	1.28
7	Norway	1.29
8	Sweden	1.32
9	Uruguay	1.38
10	Australia	1.42
11	Singapore	1.42
12	Lithuania	1.48
13	Canada	1.52
14	Saint Vincent and The Grenadines	1.52
15	Switzerland	1.52
16	Ireland	1.54
17	Dominica	1.54
18	Slovenia	1.55
19	Barbados	1.56

Vigilant Players

Rank	Country	SECI Score
20	Netherlands	1.58
21	Austria	1.61
22	Seychelles	1.61
23	Israel	1.63
24	Latvia	1.63
25	Belgium	1.63
26	France	1.65
27	United Kingdom	1.65
28	Japan	1.66
29	Germany	1.66
30	Saint Lucia	1.68
31	Korea, South	1.68
32	Czech Republic	1.68
33	Chile	1.69
34	Grenada	1.72
35	Portugal	1.74
36	Armenia	1.74
37	Botswana	1.75
38	Bhutan	1.76
39	Bahamas	1.77
40	Greece	1.78
41	Georgia	1.79
42	Poland	1.80
43	Vanuatu	1.82
44	Fiji	1.83

Rank	Country	SECI Score
45	United States	1.85
46	Cyprus	1.86
47	Spain	1.87
48	Mauritius	1.87
49	Slovakia	1.88
50	Costa Rica	1.88
51	Cape Verde	1.9
52	Namibia	1.95
53	Oman	1.96
54	Croatia	1.97
55	Trinidad and Tobago	1.97
56	Montenegro	1.98
57	Jordan	1.98
58	North Macedonia	1.98
59	Sao Tome and Principe	1.99
60	Albania	1.99
61	Rwanda	2.00
62	Bahrain	2.01
63	Kazakhstan	2.02
64	Italy	2.02
65	Romania	2.02
66	Timor-Leste	2.03
67	Qatar	2.05
68	Tunisia	2.05
69	Moldova	2.07
70	Cuba	2.09
71	Malta	2.10
72	Hungary	2.10
73	Jamaica	2.11
74	Argentina	2.11
75	Morocco	2.14
76	Mongolia	2.14
77	United Arab Emirates	2.14
78	Bulgaria	2.15
79	Dominican Republic	2.17
80	Saudi Arabia	2.18
81	Zambia	2.19
82	Malaysia	2.21
83	Senegal	2.22

Reactive Reformers

Rank	Country	SECI Score
84	Ghana	2.23
85	Gambia	2.23
86	Malawi	2.25
87	Serbia	2.25
88	Bosnia and Herzegovina	2.27
89	Egypt	2.27
90	Lesotho	2.28
91	Sri Lanka	2.28
92	Uzbekistan	2.28
93	Guyana	2.29
94	Peru	2.31
95	Solomon Islands	2.31
96	India	2.31
97	Kuwait	2.33
98	Suriname	2.33
99	Maldives	2.35
100	Colombia	2.35
101	Ethiopia	2.35
102	Burundi	2.36
103	Bolivia	2.36
104	Ukraine	2.36
105	Indonesia	2.38
106	Benin	2.39
107	Ecuador	2.41
108	Azerbaijan	2.41
109	Brazil	2.42
110	Belarus	2.42
111	El Salvador	2.43
112	Tanzania	2.43
113	South Africa	2.43
114	Cote D'ivoire	2.44
115	Mauritania	2.46
116	Djibouti	2.47
117	Bangladesh	2.47
118	Pakistan	2.48
119	Burkina Faso	2.49
120	Türkiye	2.49
121	Sierra Leone	2.51
122	Philippines	2.51
123	Paraguay	2.53
124	Kyrgyzstan	2.53
125	Guatemala	2.53
126	Guinea	2.53
127	Thailand	2.53
128	Nepal	2.53
129	Togo	2.54
130	Panama	2.55
131	Uganda	2.57
132	Eswatini	2.58
133	Algeria	2.58
134	Mexico	2.59
135	Zimbabwe	2.59
136	Comoros	2.61
137	Angola	2.62
138	Niger	2.63
139	Vietnam	2.64
140	Honduras	2.64
141	Papua New Guinea	2.65
142	Russia	2.66
143	China	2.66
144	Lebanon	2.68
145	Madagascar	2.70
146	Turkmenistan	2.70
147	Tajikistan	2.71
148	Mali	2.72
149	Cameroon	2.74
150	Liberia	2.75
151	Eritrea	2.76
152	Kenya	2.76
153	Gabon	2.77
154	Republic of the Congo	2.77
155	Nicaragua	2.78
156	Lao PDR	2.81
157	Guinea-Bissau	2.82
158	Mozambique	2.84
159	Equatorial Guinea	2.84
160	Nigeria	2.85
161	Cambodia	2.86

Regulatory Laggards

Rank	Country	SECI Score
162	Iraq	2.86
163	Chad	2.92
164	Sudan	2.93
165	Korea, North	2.94
166	Central African Republic	2.96
167	Syrian Arab Republic	2.99
168	Libya	3.01
169	Yemen	3.06
170	Haiti	3.08
171	Somalia	3.09
172	Iran	3.09
173	Democratic Republic of the Congo	3.11
174	Venezuela	3.15
175	Afghanistan	3.21
176	South Sudan	3.26
177	Myanmar	3.31

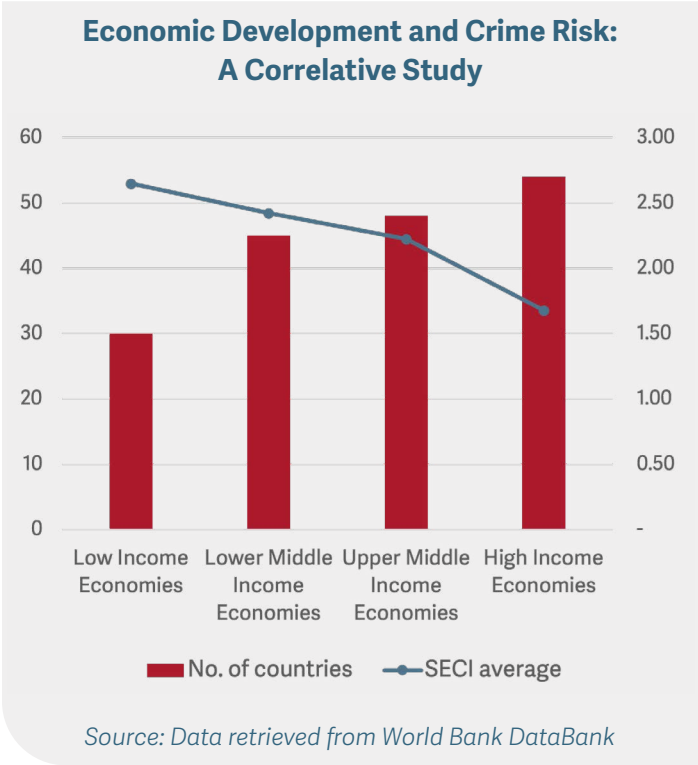
GNI and SECI: Unveiling the Relationship Between Income Levels and Economic Crime Risk

We have analyzed the correlation between a country's income level and its exposure to economic crime risk using the latest available Gross National Income per capita (GNI) for each country from the World Bank. Countries were grouped according to the World Bank's official economic classifications, as follows:

- Low-income (GNI ≤ USD 1,145);
- Lower-middle-income (GNI between USD 1,146 – USD 4,515);
- Upper-middle-income (GNI between USD 4,516 – USD 14,005); and
- High-income (GNI > USD 14,005).

Mapping these classifications against SECI scores reveals important trends. Lower-income economies generally exhibit higher SECI scores, indicating greater exposure to both financial and economic crime risks. However, it is essential to recognize the distinct ways in which economic crime manifests across different income groups.

The following chart highlights these patterns by plotting the number of countries in each income category against their average SECI risk scores. The trend suggests that as income levels rise, SECI risk scores tend to decrease, reflecting stronger regulatory controls and institutional frameworks.



Source: Data retrieved from World Bank DataBank

This analysis underscores how institutional strength, regulatory effectiveness, and economic development shape a country's exposure to financial and economic crime.

Lower-income and weaker governance environments tend to be more vulnerable at the placement stage of illicit financial flows, as gaps in enforcement and oversight create entry points for proceeds of crime. These jurisdictions may also face higher risks of predicate offenses, such as corruption, human trafficking, and illicit trade, which fuel broader financial and economic crimes.

Conversely, higher-income and cross-border financial centers often play a more significant role in the layering and integration stages, where illicit funds are moved and legitimized through sophisticated structures, including trade-based schemes, shell entities, and complex financial instruments. These economies may exhibit lower SECI risk scores overall due to stronger regulatory controls, but they remain critical nodes in global illicit finance networks.

Understanding the Relationship Between SECI and Government Effectiveness

Governance quality is a fundamental determinant of a country's financial crime risk exposure. To examine this relationship, we compared SECI with the Government Effectiveness Index (latest available on the World Bank website),[1] which measures the quality of public services, policy implementation, and institutional strength. The bubble chart below visualizes this relationship, with SECI scores on the X-axis, Government Effectiveness Index scores on the Y-axis, and bubble sizes representing economic scale or population weight. The results reveal a strong inverse correlation between government effectiveness and financial crime risk.

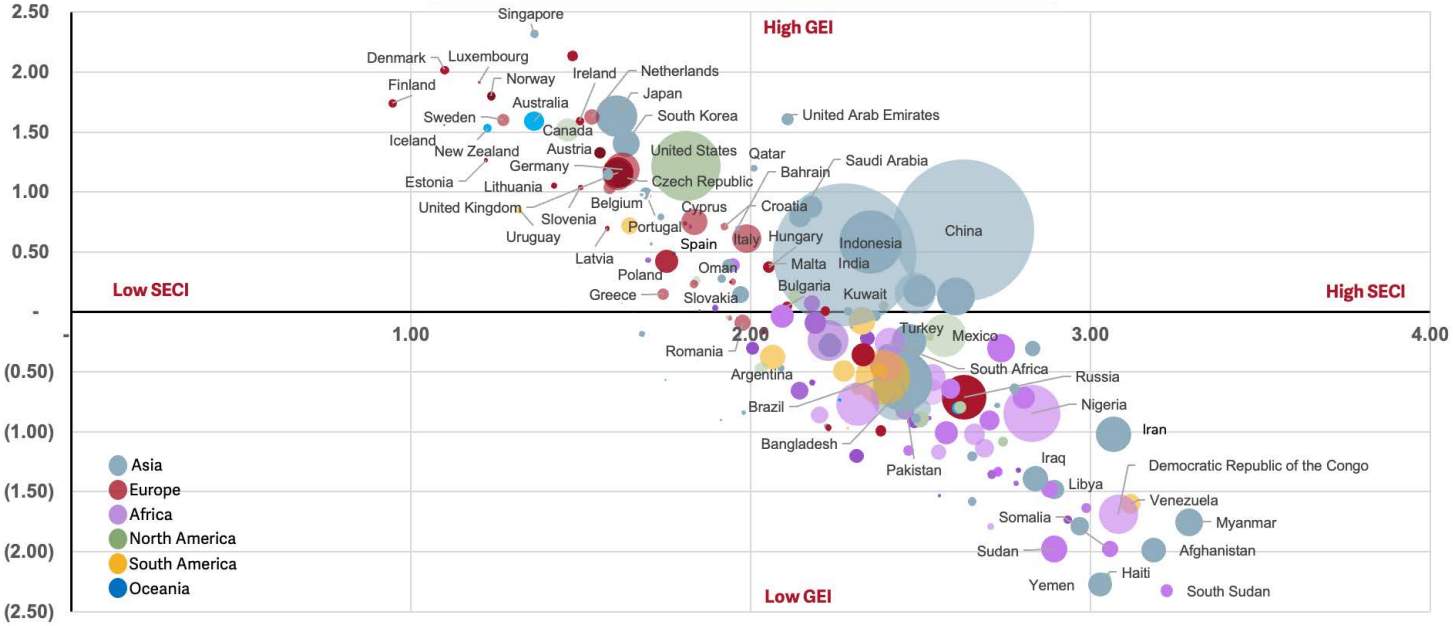
Countries with weak governance structures tend to have high SECI scores, indicating greater exposure to systemic financial crime risks due to poor institutional controls, regulatory inefficiencies, and corruption vulnerabilities.

- **Myanmar, South Sudan, Afghanistan, Venezuela, Democratic Republic of the Congo, Somalia, Haiti, Yemen, and Libya**: These nations exhibit extremely high SECI scores and low governance effectiveness, driven by political instability, high corruption, and weak financial oversight.

Beyond these, certain high-risk countries also notably stand out due to their significant share of the global population:

- **Nigeria, Pakistan, and Bangladesh:** Large populations with governance challenges contribute to higher risks of money laundering and illicit financial flows.

Exploring the SECI-Government Effectiveness Nexus Across Key Countries



Source: DataBank, WorldBank

1 Worldwide Governance Indicators, World Bank.

- **Iran and Iraq**: Weak institutional oversight, political interference in financial regulation, and reliance on informal financial networks undermine AML enforcement, fostering systemic financial crime risks.
- **Russia:** War-related sanctions, state-controlled financial networks, and a shift to informal payment systems have weakened regulatory oversight, increasing vulnerability to financial crimes.

Conversely, countries with strong governance frameworks generally exhibit lower SECI scores, reflecting more effective financial regulation, stronger enforcement mechanisms, and greater economic stability.

- **Finland, Denmark, Iceland, Norway, Luxembourg, and Sweden**: These high-income economies rank among the best-governed nations with strict financial regulations and low corruption levels.
- **Australia and New Zealand**: Robust governance frameworks and effective AML policies ensure that financial crime risks remain minimal.
- **Singapore:** A global financial hub with strict AML regulations, Singapore maintains one of the world's lowest corruption levels through strong regulatory oversight.
- **Uruguay:** Strong governance, low corruption, and stringent AML regulations make Uruguay one of Latin America's most financially transparent countries.

While strong governance typically correlates with lower economic crime risks, certain financial hubs defy this trend. These jurisdictions maintain high governance effectiveness yet exhibit higher-than-expected SECI scores, largely due to their exposure to illicit financial flows and regulatory vulnerabilities.

- **United Arab Emirates, Qatar, and Hong Kong**: While they have strong governance, their status as financial hubs make them susceptible to illicit financial flows.
- **Malta and Cyprus**: These countries are small but financially significant jurisdictions that have faced scrutiny over money laundering and offshore banking risks.

Additionally, we note that population size also plays a significant role in shaping a country's economic crime risk profile. Larger economies with vast populations often face heightened challenges in financial crime regulation due to the scale and complexity of economic activities.

- **India:** India has a slightly higher SECI score, reflecting ongoing financial crime risks due to corruption and regulatory gaps despite a developing governance structure.
- **China:** China has a moderate SECI score despite high governance effectiveness, suggesting that strict regulatory enforcement mitigates risks, but financial secrecy laws still pose challenges.
- **Indonesia:** Another large population country with moderate SECI and governance effectiveness, Indonesia highlights the complexity of financial oversight in emerging economies.
- **Pakistan**: Pakistan's high SECI score reflects persistent financial crime risks driven by corruption, weak regulatory enforcement, and a large informal economy that complicates AML efforts.

As financial crime threats continue to evolve, we must also look ahead to emerging trends shaping the 2025 financial crime landscape. Several key developments are expected to redefine risk management, compliance, and regulatory strategies in the coming months. Understanding these trends is crucial for businesses, regulators, and financial institutions as they prepare for a rapidly changing compliance landscape throughout 2025 and beyond.

Global Financial and Economic Crime Outlook

2025 KEY TRENDS

1

DISRUPTIVE AI TECHNOLOGY AND DEEPFAKE FRAUDS

AI-driven deepfake technologies are enabling sophisticated impersonation and fraud, challenging identity verification systems.

2

VIRTUAL ASSETS RISKS

Cryptocurrencies introduce new risks, including anonymity and cross-border transfer complexities, requiring enhanced monitoring.

3

REAL-TIME TRANSACTION MONITORING

Advanced systems analyze transactions instantly to detect anomalies, enabling faster responses to potential financial crimes.

4

REGULATORY TECHNOLOGY (REGTECH) INTEGRATION

RegTech solutions streamline compliance by automating KYC, AML, and reporting processes with higher accuracy.

5

LEVERAGING BEHAVIORAL BIOMETRICS FOR ADVANCED FRAUD DETECTION AND PREVENTION

Behavioral analytics track user patterns to detect fraudulent activities with greater precision.

6

PROLIFERATION FINANCING

Illicit funding of Weapons of Mass Destruction (WMD) programs is a growing concern, necessitating targeted sanctions and compliance measures.

7

CONVERGENCE OF SANCTIONS AND AML/CFT GOVERNANCE

Sanctions evasion is now a key financial crime risk, pushing regulators to integrate AML/CFT efforts for a unified, intelligence-driven approach. Sanctions are now central to global crime enforcement.

8

RISE OF WHITE-COLLAR FRAUDS AND EXTERNAL THREATS

Increased financial crimes within organizations demand robust corporate governance and internal controls.

9

CROSS-BORDER DATA SHARING

Global collaboration on financial data is crucial for combating transnational financial crimes effectively.

10

FOCUS ON ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG) FACTORS

ESG considerations are increasingly integrated into FCC to address issues like human trafficking and corruption.

1

Disruptive AI Technology and Deepfake Frauds: Enhancing Compliance While Amplifying Financial Crime Risks

The rise of disruptive AI and deepfake fraud is significantly increasing financial crime risks, with a projected 55–60% increase in incidents by the end of 2025.

Our observations align with industry findings that highlight the increasing sophistication of AI-powered fraud, ranging from deepfake-enabled identity theft to large-scale automated scams.

The advent of faster payment systems, such as real-time payments and same-day Automated Clearing House (ACH), combined with advancements in AI technology, has led to a noticeable increase in Authorized Push Payment (APP) fraud. Criminals exploit the speed of funds movement, convincing victims to authorize transactions under false pretenses. The victim is persuaded to make the transfer voluntarily, often under the belief that it is a legitimate transaction (e.g., paying a supplier, making an investment, or sending money to a friend). Countries like the United Kingdom are already responding with targeted policies to combat APP fraud, a regulatory trend expected to gain traction globally.

Deepfake technology, combined with AI, enables fraudsters to impersonate high-value customers or executives, authorizing illicit transactions or generating realistic messages from CEOs to deceive employees into transferring funds or sharing sensitive data. It is also used in social engineering attacks, manipulating victims emotionally, and for identity theft, which can lead to financial fraud, online scams, or the creation of fake accounts.

A notable example occurred in 2024 when Arup, a United Kingdom (UK)-based engineering firm, fell victim to a deepfake fraud. Fraudsters impersonated the company's Chief Financial Officer (CFO) and other employees during a video conference. Believing the communications to be legitimate, a staff member authorized 15 transactions totaling HKD 200 million (approximately USD 26 million) to accounts in Hong Kong.[2]

From a compliance perspective, AI-driven solutions offer a critical defense by enabling real-time anomaly detection, proactive risk assessments, and enhanced fraud monitoring. As financial crime techniques evolve, institutions must leverage AI not only as a tool for detection but also as a strategic component of their broader risk management frameworks.

2 CNN, 2024. Arup hit by deepfake scam, loses USD 25 million to fraudsters.

Authorized Push Payment (APP) fraud

Scammer identifies a target

Tactics used include phishing, impersonation, or social engineering.

Victim initiates a transaction

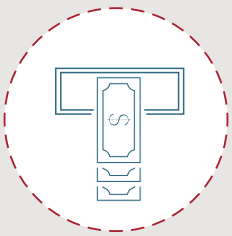
Under deception, the victim initiates the transaction, believing the transaction is legitimate.

Payment is transferred

The payment is processed through instant payment networks or real-time settlement systems.

Funds land in the fraudster's account

The fraudster secures the funds in their controlled account, often using mule or intermediary accounts.



Money is laundered or withdrawn

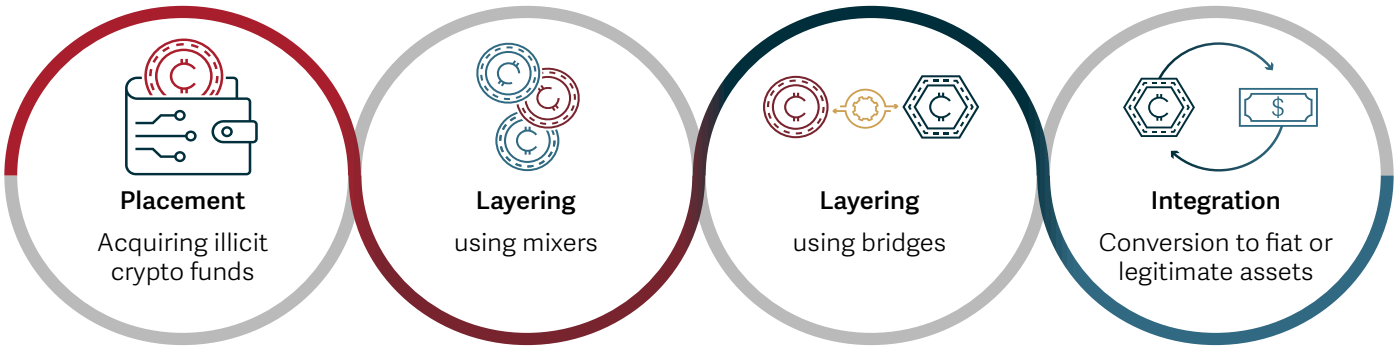
Layering techniques are used to make the recovery difficult.

2

Virtual Assets Risks: Fraud, Money Laundering, and the Need for Stronger Oversight

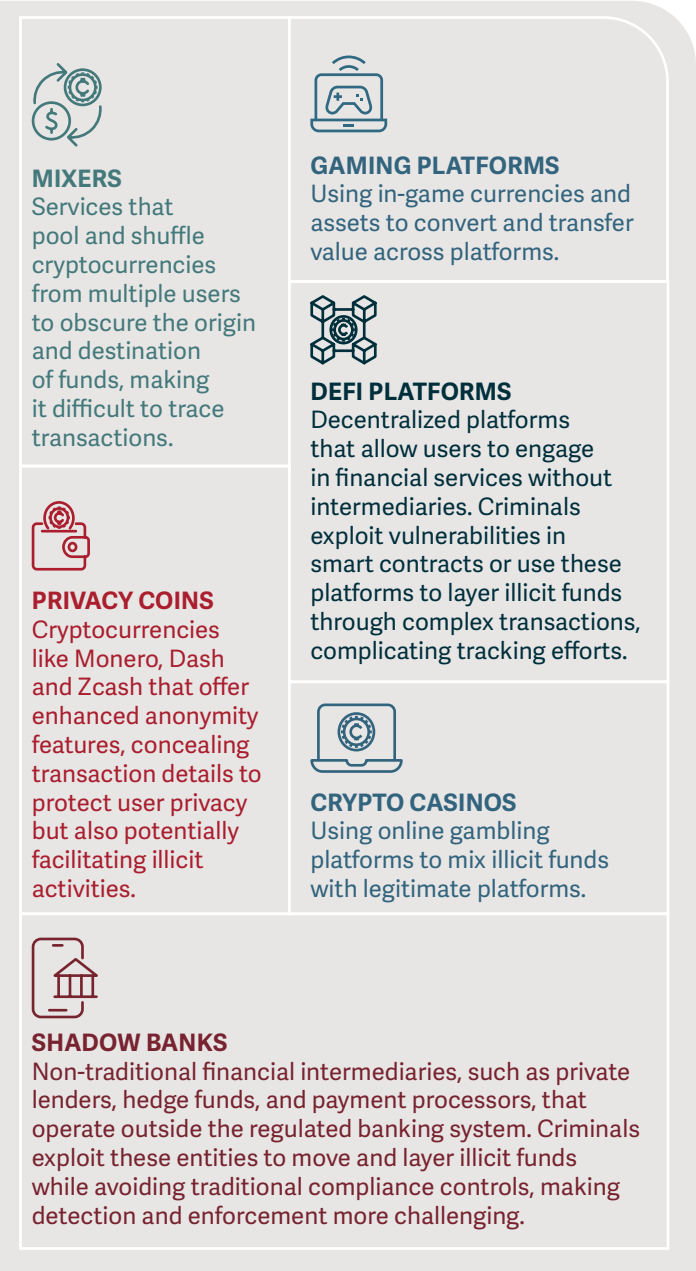
While virtual assets are reshaping global finance, they have also introduced complex financial crime risks that continue to escalate, including — but not limited to — fraud, money laundering, and terrorism financing fraud, money laundering, and terrorism financing. The 2023 Cryptocurrency Fraud Report published by the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) reported total losses from crypto fraud amounting to USD 5.6 billion which was a 45% increase compared to 2022.[3] We anticipate cyber-related frauds to surpass USD 100 billion by 2030, as adoption accelerates, financial criminals will continue to exploit gaps in regulation and compliance. In response, we expect regulators to intensify oversight, financial institutions to adopt more sophisticated blockchain analytics, and cross-border collaboration to become a critical defense mechanism against crypto-enabled financial crime.

Over the years, we have observed that criminals are leveraging increasingly sophisticated techniques to obscure the origins of illicit funds, using mixers and bridges before integrating them into legitimate financial systems. The diagram below illustrates a typical on-chain laundering workflow, progressing through four stages: placement (illicit crypto), layering (crypto mixers and crypto bridges), and integration (legitimate financial system).



3 FBI, 2023 Cryptocurrency fraud report released

Money laundering operations involving virtual assets are often highly complex, employing mixers, cross-chain bridges, and intermediary wallet hops to obscure the origins and movements of illicit funds. Cybercriminals leverage several platforms to layer illicit funds. In our experience, some of the techniques used by cybercriminals for layering illicit funds are mentioned in the image below.



The decentralized nature of virtual assets complicates transaction tracking and enables cross-border financial flows, as highlighted by the 2022 FTX collapse. This has led to increased scrutiny from regulators like the US Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC), requiring financial institutions involved in virtual assets to adopt stronger compliance measures. Fraud has surged, with cases like the 2023 Atomic Wallet breach, where over USD 100 million was stolen by the North Korean Lazarus group. These incidents exploit the lack of trust in crypto platforms, increasing risks for users.[4]

We expect regulatory scrutiny on virtual assets to intensify throughout 2025, driven by initiatives such as FATF's Travel Rule and national regulations like the Financial Crimes Enforcement Network (FinCEN) in the US and the Markets in Crypto-Assets Regulation (MiCA) in the European Union (EU).

Furthermore, we note that the US Treasury's 2024 National Strategy for Combating Terrorist and Other Illicit Financing focused on strengthening the AML/Countering the Financing Of Terrorism (CFT) framework. Key priorities include closing regulatory gaps, improving law enforcement effectiveness, and supporting responsible technological innovation to reduce illicit finance risks.[5]

4 Reuters, 2024. North Korean hackers sent stolen crypto wallet used by Asian payment firm.

5 US Department of the Treasury, 2024 Illicit Finance Strategy.

3

The Critical Role of Real-Time Transaction Monitoring in Financial Crime Protection

Real-Time Transaction Monitoring (RTTM) actively monitors and analyzes financial transactions in real-time to identify inconsistencies, suspicious patterns, or illegal activities. It mitigates fraud risks by triggering instant due diligence for high-risk transactions exceeding predefined thresholds, improving fraud detection, resolution speed, and customer service while reducing false positives.

RTTM also helps ensure data privacy is not compromised as it instantly flags the transaction, taking away the need for compliance teams to communicate over non-secure channels like email if they use different information systems and eliminates the need for retrospective investigation(s).

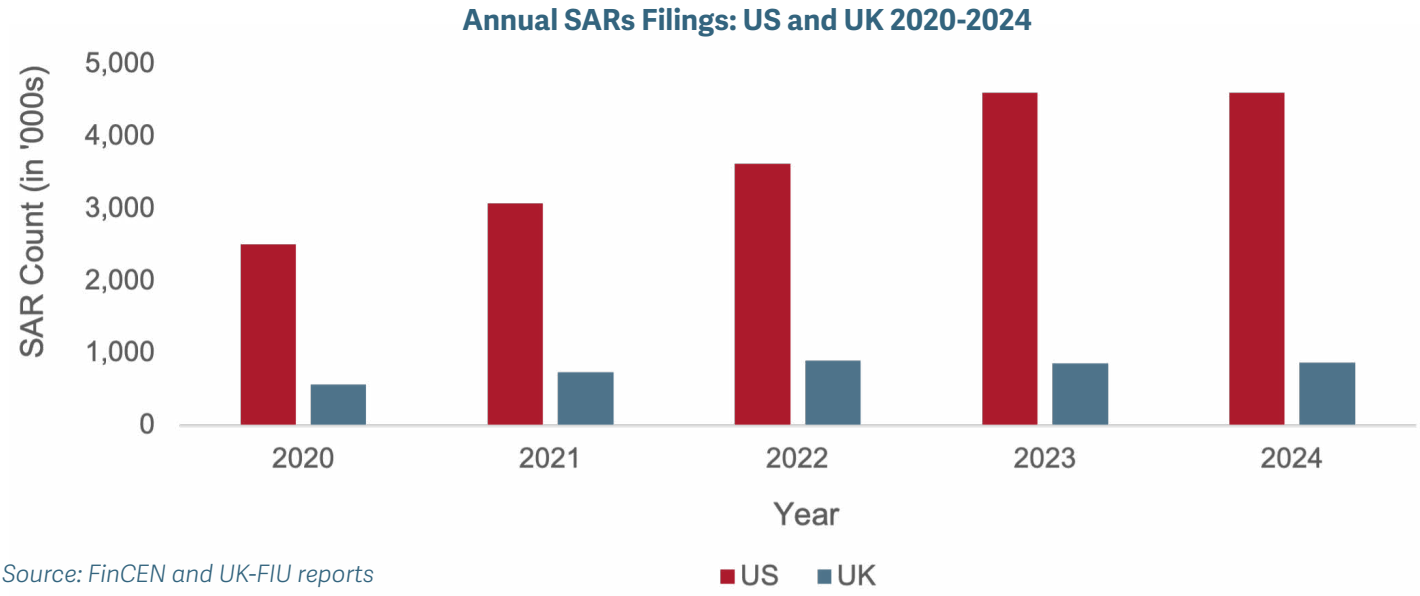
Integration of RTTM with advanced analytics capabilities and AI revolutionizes fraud detection by spotting anomalies, adapting to new threats, and cutting false positives with precision.

As financial crime becomes increasingly sophisticated, the volume of flagged transactions continues to grow, making Suspicious Activity Reports (SARs) a critical tool for regulatory oversight. According to FinCEN, approximately 4.6 million SARs were filed in the US in 2023 — equating to nearly 12,600 reports per day.[6] The majority of these were submitted by depository institutions and money services businesses (MSBs). Notably, there was a significant uptick in SARs related to check fraud and elder financial exploitation. Over recent years, FinCEN has consistently reported a sustained upward trend in SAR filings.

In the UK, a similar pattern emerged. The UK Financial Intelligence Unit (UK-FIU) recorded 872,048 SARs in its latest SARs Annual Report 2024 (covering April 2023 through March 2024), reflecting a 1.5% increase from the previous reporting period.[7] This steady growth underscores the expanding role of SARs in identifying and mitigating financial crime risks.

6 Financial Crimes Enforcement Network (FinCEN), SAR Stats.

7 National Crime Agency, SARs annual report 2024.



Source: FinCEN and UK-FIU reports

The continued rise in SAR volumes globally is in part driven by increasingly sophisticated RTTM tools. These systems are evolving rapidly, enabling faster, more accurate detection of suspicious activity and strengthening institutions' ability to report potential financial crime with greater precision.

4

RegTech Revolutionizing Compliance Infrastructure Empowered by AI Integrations

Regulatory Technology (RegTech) simplifies compliance by bridging financial institutions and regulatory bodies, improving risk assessment by analyzing large datasets and proactively identifying vulnerabilities. It also supports real-time risk scoring, sanctions screening, and customer identity verification, with cloud-based platforms enhancing global compliance and reducing manual labor.

If RegTech is integrated with other tools like Blockchain, it enhances transparency and data integrity, providing a source and repository of secure, immutable records of transactions. The combination of RegTech and Blockchain-based solutions are expected to become more prevalent for Know-Your-Customer (KYC), Know-Your-Transaction (KYT) and AML processes, offering enhanced security and efficiency in identity verification and transaction monitoring. AI and machine learning further enhance RegTech's capabilities by continuously refining risk models, detecting emerging threats, and adapting to evolving regulatory requirements.

We have observed that RegTech can improve compliance by reducing false positives through advanced analytics, real-time monitoring, automation, smart ID verification, and enhanced risk assessments. These techniques have boosted the accuracy of KYC processes, sanctions screening, transaction monitoring, and financial crime reporting.[8]

The UK Financial Conduct Authority (FCA) defines RegTech as "a subset of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities."[9]

Increase in the Implementation of RegTech Solutions

> "78% of Jersey firms believe RegTech tools are increasingly necessary for acheiving compliance."

Source: Jersey Financial Services Commission, July 2022

8 Silent Eight, 2025 Trends in AML and Financial Crime Compliance.

9 Thompson Reuters Regulatory Intelligence Report of 2023.

HSBC, a major universal bank and financial services group, is a key example of RegTech adoption. HBSC uses Featurespace's ARIC platform for automated transaction monitoring, which improves efficiency, reduces false positives, and enhances suspicious activity detection. By implementing this solution, HSBC significantly reduced manual labor and improved alert quality, making its compliance processes more efficient and scalable. However, the implementation faced challenges, including ensuring data quality and security, especially when using cloud technology for sensitive AML data. HSBC had to invest heavily in reviewing and updating its data infrastructure and collaborate closely with Featurespace to align regulatory requirements with ARIC's capabilities. These efforts helped overcome integration challenges and ensured that the platform met the stringent standards of the financial industry.

Secretariat's view is that while RegTech offers significant advantages, overreliance on the technology may potentially sideline the nuanced judgment and ethical considerations that only human expertise can offer. Relying heavily on a single system without adequate backups can also heighten the risk of critical failures, even from minor issues or errors within the system.

5

Leveraging Behavioral Biometrics for Advanced Fraud Detection and Prevention

Unlike traditional biometrics like passwords and fingerprints, which are static, behavioral biometrics analyze how users interact with devices. This includes typing rhythm, mouse movements, and touchscreen pressure, enabling authentication and fraud detection. This helps improve fraud detection methods by detecting anomalies in real time and combating identity theft and account takeovers before they escalate.

In our experience, behavioral biometrics have proved to be useful in identifying cases of account takeover where the cybercriminals start behaving differently than the legitimate account holder.

One potential cause for failure is that variations in behavior over time due to external factors like stress, device changes, and injury can negatively impact detection accuracy and flag false positives. Compliance with data protection laws also becomes a significant issue with statutes like the General Data Protection Regulation (GDPR). GDPR focuses on securing data privacy and individual protection, making legal adherence a task when balancing monitoring and user privacy.

A notable example showcasing the importance of behavioral biometrics is IBM's integration of this technology in its Trusteer Pinpoint Detect platform. The platform uses cognitive analytics and machine learning to identify subtle behavioral patterns that may signal fraud, such as changes in typing rhythm or inconsistent cursor movement. The implementation has significantly improved fraud detection rates while minimizing false positives. Financial institutions leveraging this technology have seen enhanced customer protection, particularly against sophisticated threats like account takeovers and authorized payment fraud. However, challenges remain, including the need to ensure customer privacy, achieve seamless integration with existing security frameworks, and reduce the computational demands of real-time analytics. Despite these hurdles, we expect behavioral biometrics to continue gaining traction as a critical component of modern fraud prevention strategies.

6

Proliferation Financing Revealing the Financial Networks Behind Global Security Threats

Proliferation financing (PF) is a relevant global financial crime trend gaining attention worldwide. It refers to the use of financial systems to fund the proliferation of weapons of mass destruction (WMDs), often involving complex networks of transactions and entities. This trend is driven by international sanctions regimes, cross-border illicit trade, and evolving threats tied to geopolitical tensions.

Countries are required to implement targeted financial sanctions to comply with United Nations Security Council (UNSC) resolutions on the financing of WMD proliferation. This obligation includes the immediate freezing of assets and funds associated with individuals or entities designated by the UNSC for their involvement in the illicit spread of WMDs and domestic cooperation.

International regulatory bodies have identified PF as a critical global concern and are pushing for its integration into AML and CFT frameworks. The FATF has initiated several measures to combat PF in 2024-2025. These include a public consultation on changes to Recommendation 16 regarding wire transfers, new guidance on trusts, and efforts to implement standards for virtual asset service providers (VASPs). The FATF has expressed concern about Russia's growing financial ties with North Korea and Iran, thereby increasing risks associated with PF.[10]

In 2024, several nations took significant steps to address PF. For instance:

- The United States' 2024 National Proliferation Financing Risk Assessment notes persistent efforts by PF networks to exploit the US financial system. The assessment also identifies VASPs as potentially vulnerable to PF networks due to compliance deficiencies.[11]
- The UAE's Executive Office of Anti-Money Laundering and Counter-Terrorism Financing (EOCN) issued guidance on Proliferation Financing Institutional Risk Assessment for Financial Institutions, Designated Non-Financial Businesses and Professions (DNFBPs), and VASPs in 2024.[12]
- Singapore's 2024 Proliferation Financing National Risk Assessment highlights that from 2019 to 2023, there were successful prosecutions of 22 individuals and eight entities for PF-related activities.[13]
- Japan released its National Risk Assessment of Proliferation Financing in June 2024, analyzing the PF risks faced by the country considering recent regulatory changes.[14]

We foresee that as more countries across Europe, Asia, and the Americas continue to strengthen their frameworks to detect, disrupt, and prevent PF, the global financial ecosystem will become increasingly interconnected in combating this evolving threat.

10 US Department of the Treasury, 2024. Press Release: jy2120; US Department of the Treasury, 2024. Press Release: jy2678.

11 US Department of the Treasury, 2024. 2024 National Proliferation Financing Risk Assessment.

12 UAE International Economic Crime Commission, 2024

13 Accounting and Corporate Regulatory Authority, 2024. Proliferation Financing National Risk Assessment. Accounting and Corporate Regulatory Authority.

14 Ministry of Finance, Japan, 2024. AML/CFT Policy.

7

Convergence of Sanctions and AML/CFT Governance

Sanctions evasion has evolved into a systemic financial crime risk, forcing regulators to rethink traditional compliance frameworks. Illicit actors, from terrorist groups to transnational criminal networks, are exploiting trade routes, opaque corporate structures, and financial loopholes to bypass sanction-driven restrictions. The 2025 Global AFC Threats Report (ACAMS) ranks sanctions and export control evasion as the second-largest global financial crime threat, underscoring its rapid rise.

In 2023 alone, Moody's Grid reported a 114% surge in sanctions evasion cases,[15] while OFAC imposed a record USD 1.5 billion in penalties in the same year.[16] This escalation — amplified by the US' recent sanctions on Chinese and Mexican cartels — demands a shift in strategy, where AML and sanctions enforcement merge into a single, intelligence-driven compliance approach.

The Evolution of Global Sanctions Frameworks

THEN (2000): A FRAGMENTED LANDSCAPE

Historically, sanctions regimes were fragmented and had a limited scope. In 2000, the United Nations (UN) focused on a few high-profile threats, such as the Taliban (harboring Al-Qaeda). The US maintained targeted sanctions against terrorism and narcotics trafficking, focusing on designated foreign terrorist organizations (FTOs) and regimes within the Middle East and on drug cartels in Colombia.

Meanwhile, the EU implemented UN Security Council's resolutions (such as the Taliban asset freezes) and maintained a few of its own restrictive measures against pariah regimes (for instance, an EU arms embargo on Myanmar and sanctions on the Milosevic government in Yugoslavia). But the EU had not yet developed autonomous sanctions regimes to address themes such as human rights or corruption globally. The UK, as an EU member, followed the sanctions imposed by the EU and implemented the UN's measures through national regulations, without an independent sanctions policy of its own.

2010–2024: PUSH FOR GLOBAL ALIGNMENT

In the 2010s, a global shift toward broader and more coordinated sanctions efforts was observed. The US expanded its sanctions framework to target organized crime and terrorism aggressively. The introduction of Magnitsky-style sanctions linked human rights violations and corruption directly to asset freezes, an initiative quickly implemented by US allies. Similar to the US, the EU also adopted more autonomous sanctions programs, notably targeting human rights abuses and corruption. By the mid-2010s, sanctions imposed by the Western allies were more homogenous for terrorism, money laundering, and corruption. The convergence of sanctions with AML efforts marked a crucial turning point, creating a unified front in the fight against global financial crime.

NOW (2025): A UNIFIED GLOBAL APPROACH

By 2025, global sanctions frameworks have undergone a significant evolution and are largely standardized across the UN, US, EU, and UK to target key AML/CFT risk areas. Today, these regimes align on imposing sanctions against terrorism, WMD proliferation, narcotics trafficking, organized crime, human rights violations,

15 Moody's, 2024. Sanctions Compliance & Sanctions Evasion: Increased Enforcement and Evolving Tactics.

16 Moody's, 2024. Sanctions Compliance & Sanctions Evasion: Increased Enforcement and Evolving Tactics.

and corruption. A notable development in 2025 was the designation of Mexican drug cartels as FTOs by the US, expanding counterterrorism laws to target the cartels' financial networks and increasing compliance burdens on financial institutions. Similarly, the UK introduced sanctions targeting organized crime, while the EU moved forward with draft legislation against corruption, demonstrating a growing consensus that sanctions are now a core AML tool.

The Overlap Between Sanctions and AML/CFT Compliance

For years, sanctions and AML compliance operated in silos. Traditionally, sanctions have been a tool for enforcing national security objectives, restricting financial transactions with designated individuals and entities. Meanwhile, AML/CFT frameworks focus on preventing financial crimes by ensuring transparency in financial transactions. However, in practice, both systems intersect — criminal networks, corrupt officials, and sanctioned entities often rely on similar tactics, including the use of shell companies, opaque financial structures, third-party intermediaries, and complex trade-based money laundering schemes, to evade detection.

Shared Compliance Pillars and Emerging Best Practices

In response, regulators are noted to focus on creating shared compliance pillars, including KYC/Customer Due Diligence (CDD), risk assessments, and internal controls, and monitoring common red flags, such as shell companies, third-party intermediaries, and unexplained transactional spikes. With the rapid expansion of US and global sanctions regimes, financial institutions must move beyond a checkbox approach to AML — compliance teams must now fuse financial intelligence with geopolitical risk analysis to anticipate evolving sanctions risks and effectively disrupt evasion networks.

Sanctions are no longer just foreign policy levers. They are central to global financial crime enforcement, used to isolate bad actors, dismantle illicit networks, and protect the integrity of the international financial system.

AML Predicate Offenses and Sanctions Convergence: 2000 vs 2025

	Then (2000)				Now (2025)			
Predicate Offense	**UN**	**US**	**EU**	**UK**	**UN**	**US**	**EU**	**UK**
Terrorism	✔ (Al-Qaeda / Taliban)	✔ (Select Middle East groups)			✔	✔	✔	✔
WMD Proliferation					✔	✔	✔	✔
Narcotics Trafficking		✔ (Colombia)				✔*	✔*	✔*
Organized Crime					✔	✔	✔*	✔*
Human Rights Violation					✔	✔	✔	✔
Corruption						✔	✔	✔

*Note: EU and UK narcotics trafficking sanctions target Syria. In early 2025, the UK announced intent to create organized crime sanctions for human smuggling, while the EU proposed a 2023 law for corruption-related sanctions.

8

Rise of White-Collar Frauds and External Threats

As financial crime evolves, key fraud trends are expected to continue shaping the landscape in the coming year. This section highlights prevalent and anticipated fraud patterns, offering insights into their potential impact on businesses, financial institutions, and regulatory bodies.

CYBER FRAUDS

Cyber fraud is a growing global threat, generating billions annually through techniques like AI-driven attacks (e.g., pig butchering), data breaches, ransomware, and business email compromise. The FBI's IC3 reported that organized crime groups are behind these crimes, with losses exceeding USD 37.4 billion from 2019 to 2023. We anticipate that this trend will continue to escalate as criminals harness emerging technologies and exploit new vulnerabilities. Key threats on the rise include include Distributed Denial-of-Service (DDoS) attacks, hacking, and information theft, pushing financial institutions to adopt AI-powered tools, multi-factor authentication, and cloud safeguards. In line with these growing concerns, the FATF has prioritized combating cyber-enabled fraud from 2022 to 2024, setting the stage for global efforts to address these evolving challenges.

Regulatory pressures, such as the GDPR in Europe and California Consumer Privacy Act (CCPA) in the US, are shaping cybersecurity priorities, requiring institutions to adopt proactive, tech-driven defenses against evolving fraud schemes.

BRIBERY AND CORRUPTION

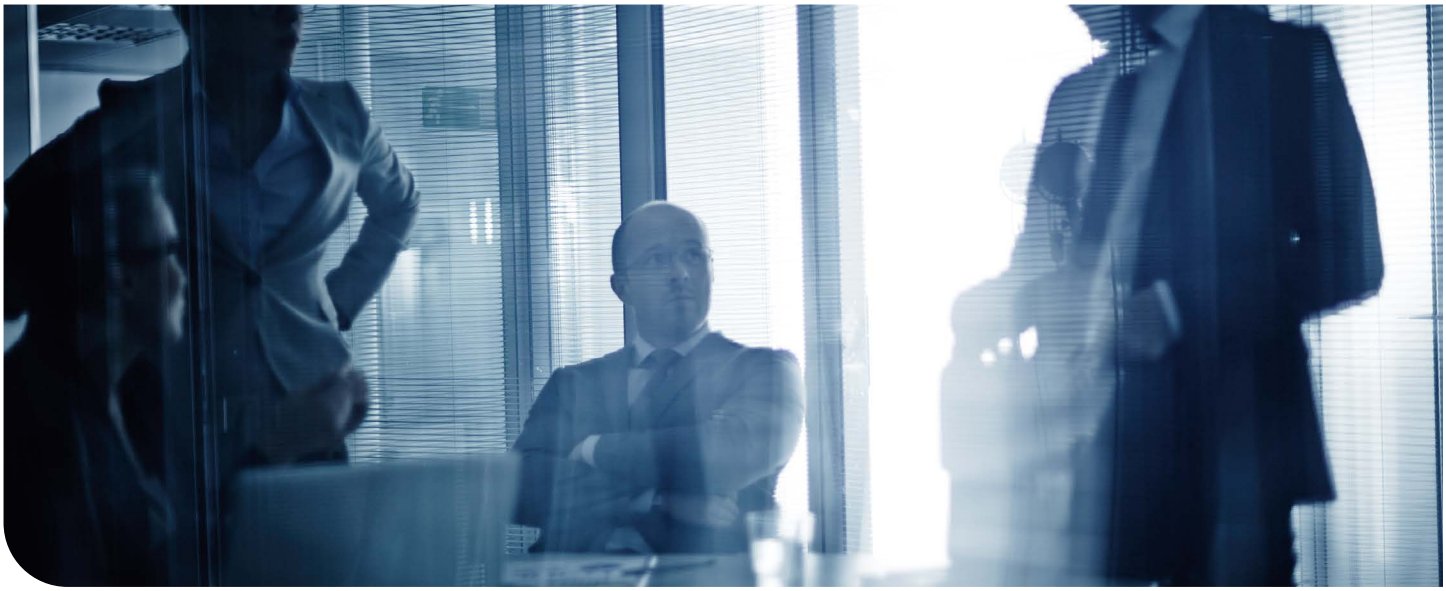
The ACFE 2024 Report to the Nations, covering 1,921 cases from 138 countries, reveals losses exceeding USD 3.1 billion, with corruption being the most common fraud type (48% of cases) and median losses of USD 200,000. The World Bank estimated that over USD 2.6 trillion, or 5% of global GDP, is lost to corruption annually[17].

Ongoing regulatory efforts, such as Australia's Crimes Legislation Amendment (Combatting Foreign Bribery) Act 2024, the UK's Economic Crime and Corporate Transparency Act 2024, the US's No Gratuities for Governing Act of 2024, and the EU's 6th Anti-Money Laundering Directive, highlight the persistent threat of bribery and corruption, which will continue to challenge economic stability and corporate integrity throughout 2025.

CORPORATE MISCONDUCT AND FINANCIAL REPORTING FRAUD

The 2023 collapse of Silicon Valley Bank (SVB) underscored broader risks associated with interest rate exposure, evolving market conditions, and the rapid spread of information through social media. This event reinforced the importance of strong board oversight in managing

17 World Bank, 2024. What are the costs of corruption?



risks and ensuring operational resilience. The collapse sparked discussions on the role of corporate governance in navigating financial challenges and maintaining stability in a dynamic environment. Meanwhile, financial statement fraud, including revenue manipulation, asset misappropriation, and improper disclosures, remains a persistent concern, as demonstrated by cases like the 2020 Wirecard fraud, where complex schemes evaded detection for extended periods.

INTERNAL VULNERABILITIES AND INSIDER THREATS

Insider threats remain a critical risk, as employees can expose sensitive information, disrupt operations, or facilitate fraud through unauthorized credit facilities, forgery, insider trading, procurement fraud, or collusion. Remote and hybrid work models have heightened vulnerabilities, increasing the risk of data breaches and phishing attacks. Advanced threats like AI-powered attacks challenge internal defenses, requiring stronger controls, better oversight, and employee training. In an era of rapid digital transformation and growing cyberattacks, ignoring insider threats can lead to severe consequences.

EVOLVING EXTERNAL THREATS

Prepaid card schemes present a growing avenue for white-collar fraud and external threats. The anonymity afforded by prepaid cards, coupled with their ease of use and global accessibility, makes them attractive tools for illicit activities. Fraudsters exploit these vulnerabilities to launder money, conceal the proceeds of crime, and facilitate unauthorized transactions. Reloadable prepaid cards, in particular, pose a heightened risk due to their ability to continuously receive funds from various sources. The absence of stringent KYC/AML controls in certain prepaid card programs further exacerbates these risks, requiring enhanced monitoring and due diligence efforts to mitigate potential abuse.

As fraud trends evolve, the landscape will continue to be shaped by cyber fraud, bribery, corporate misconduct, insider threats, and external vulnerabilities, thus requiring constant vigilance, stronger oversight, and enhanced collaboration to mitigate risk. Businesses and financial institutions must stay ahead of emerging threats by adopting proactive, tech-driven defenses.

9

Cross-Border Data Sharing

The global financial ecosystem is undergoing a transformative phase in combating financial crime, with cross-border data sharing emerging as a critical strategy. As we move through 2025, the FATF continues to lead efforts in creating uniform protocols and criteria that transcend jurisdictional boundaries, aiming to establish consistent, accurate, and accessible financial transaction data.

In recent years, some notable regulatory milestones toward international cooperation were achieved. A key development is the progress made by the United States in addressing deficiencies in its AML/CFT regime, specifically regarding FATF's Recommendation 24 (Transparency on Legal Arrangements). This progress includes the ongoing implementation of the Corporate Transparency Act, the bipartisan law that requires many companies operating in the United States to report information to the Treasury's FinCEN about who ultimately owns or controls them.[18] We expect these efforts to serve as a model for other countries, prompting further adoption of similar transparency measures.

The Economic Crime and Transparency Act 2023 (ECCTA) was also passed on 26 October 2023, introducing significant reforms to existing regulatory and corporate governance frameworks in the United Kingdom. One of the primary objectives of the ECCTA was to reform the role of Companies House, the body responsible for incorporating and maintaining companies in the United Kingdom. This reform aims to improve transparency, thereby limiting the abuse of corporate structures. While Companies House was traditionally viewed as a passive repository of information, the amendments introduced by the ECCTA give Companies House expanded powers to scrutinize and challenge information it receives. Notably, Companies House can now verify the identity of company directors and remove fraudulent entities from the company register.[19]

18 US Department of the Treasury, 2024. Press Release: jy2208

19 A closer look at recent trends reveals crackdown on money laundering in Europe — Global Investigations Review

Despite FATF recommendations urging countries to create databases of legal entities and arrangements containing information on beneficial owners, global implementation has been inadequate. The Organization for Economic Co-operation and Development's (OECD) July 2024 report, *Beneficial Ownership and Tax Transparency — Implementation and Remaining Challenges*, reported that nearly 50% of the 112 jurisdictions assessed to date have severe deficiencies in their legal framework and/or ineffective implementation of their beneficial ownership framework.[20] This indicates that as of July 2024, over 56 jurisdictions did not fully comply with FATF's initiative on Beneficial Ownership Transparency. Furthermore, a 2022 FATF report on State of Effectiveness and Compliance with FATF Standards highlighted that only 52% of 120 assessed jurisdictions have the necessary laws and regulations to understand, assess the risks of, and verify the beneficial owners or controllers of companies; moreover, only 9% of countries have effectively implemented such legislation.[21]

Countries must catch up to the rapidly evolving financial crime landscape. By sharing transparency and working together, we can unmask criminal networks and hold bad actors accountable. The call to action is clear: Strengthen cross-border collaboration and regulatory frameworks now to build a safer, more resilient global financial system.

20 OECD, 2024. Beneficial Ownership and Tax Transparency: Implementation and Remaining Challenges.

21 Financial Action Task Force (FATF), 2024. Effectiveness of Compliance with Standards.

10

ESG Key to Sustainable Financial Crime Prevention

The integration of Environmental, Social, and Governance (ESG) considerations into financial crime compliance is expected to become increasingly critical. In our view, the convergence of ESG factors with traditional compliance frameworks will reshape how organizations address financial crime risks. This evolution is likely to have a significant impact on areas such as supply chain integrity and the financing of environmentally harmful activities, driving a more robust and forward-looking approach to risk management.

Emerging Risks

Greenwashing and Fraudulent ESG Claims: The surge in ESG investing has led to instances where companies exaggerate or fabricate their sustainability efforts to attract investment. This deceptive practice, known as greenwashing, poses significant risks to investors and undermines genuine sustainability initiatives. For example, in December 2024, the Financial Times reported that global ESG funds have an estimated USD 1.4 billion invested in companies linked to forced labor in Xinjiang, raising concerns about the authenticity of ESG claims.[22]

Supply Chain Vulnerabilities: Complex, multi-tiered supply chains can obscure unethical practices, including human rights violations and environmental harm. The European Union's Corporate Sustainability Due Diligence Directive (CSDDD), adopted in July 2024, mandates companies to identify and prevent human rights abuses within their supply chains, emphasizing the need for enhanced supply chain transparency and accountability.

Why It Matters

The intertwining of ESG metrics with financial crime compliance reflects a broader recognition that ethical lapses can have severe legal, financial, and reputational repercussions. Regulatory bodies are intensifying scrutiny, and investors are increasingly prioritizing companies with robust ESG practices. Among S&P 500 companies, 77.2% linked ESG performance to their executive incentive compensation plans in 2024, down marginally from 77.8% in 2023.[23] Further, in the European markets, 90% of companies now use ESG metrics in their incentive systems, an increase of 11 percentage points over the prior year.[24]

22 Financial Times, 2024. ESG-linked executive pay is under pressure.

23 Harvard Law School Forum on Corporate Governance, 2025. ESG Performance Metrics in Executive Compensation Strategies. Harvard Law School.

24 WTW, 2023. ESG metrics in European executive incentive plans.

Legislative measures such as the EU's CSDDD and the US Uyghur Forced Labor Prevention Act are compelling companies to conduct thorough due diligence on their supply chains to prevent human rights abuses and environmental violations. Noncompliance can lead to substantial penalties and legal challenges.

Institutional investors are demanding greater transparency and accountability regarding ESG practices.

Companies failing to meet these expectations may face divestment and reputational damage. The increasing integration of ESG metrics into executive compensation underscores this trend.

A Proactive Defense Against Financial Crime for 2025 and Beyond

The escalating complexity of cyber threats, heightened regulatory scrutiny, and sophisticated criminal tactics necessitate a multi-layered, technology-driven, and globally coordinated approach to combat financial crime in 2025 and beyond. As certain jurisdictions revisit or realign their enforcement priorities, including in the area of anti-corruption, the risk of regulatory fragmentation grows. In this evolving landscape, financial institutions and regulatory bodies must adopt proactive, forward-looking risk mitigation strategies to safeguard the financial system and uphold global financial integrity.

Key Actions for 2025

1. **Embracing the Digital Sentinel: RegTech for Proactive Compliance**
   Financial institutions should leverage RegTech solutions to enhance compliance efficiency and proactively combat financial crime. Cloud-based platforms streamline global compliance, while AI-driven RTTM enables instant detection of suspicious activities. Machine learning-powered anomaly detection, behavioral biometrics, and blockchain integration strengthen fraud prevention, data integrity, and KYC/AML processes. A hybrid approach, combining automation with human expertise, ensures ethical oversight, and scalable RegTech frameworks future-proof against evolving threats.

2. **Fortifying Cybersecurity Against AI Threats**
   The rise of AI-powered cyber fraud requires robust cybersecurity frameworks. Implement multi-layered defenses, including AI-driven fraud detection, biometric authentication, and advanced anomaly detection. Combat deepfake impersonation by integrating liveness detection in identity verification. Conduct regular cybersecurity drills, including simulated phishing attacks, to educate employees. Invest in zero-trust architecture for continuous verification of users and devices.

3. **Mitigating Risks from External Counterparties**
   Address risks from overreliance on external counterparties through comprehensive third-party risk assessments. Include strict data security clauses in contracts, requiring compliance with standards like ISO 27001. Conduct regular cybersecurity audits of third-party providers. Implement robust Enhanced Due Diligence (EDD) and KYC checks for customers that are tailored to their specific risks.

4. **Intelligent Monitoring for Sanctions Evasion Prevention**
   Combat sanctions and export control evasion by integrating Risk-Based Due Diligence (RBDD) with advanced technology. Utilize AI-driven screening and monitoring to detect hidden ownership, suspicious transactions, trade-based money laundering (TBML), adverse media, and geolocation tracking. Enhance crypto compliance with blockchain analytics and use maritime risk intelligence to uncover vessel identity tampering.

5. **Internal Accountability and Governance**
   Strengthen internal governance and accountability. Hold leadership responsible for compliance, embed a compliance culture, and establish whistleblower protection. Conduct regular financial crime training, red teaming simulations, and risk assessments. Develop incident response plans and foster a compliance-driven environment to reduce internal fraud and misconduct.

Even the most robust defenses cannot eliminate risk entirely. When a crisis hits, institutions must react, respond, and remediate to minimize impact, restore trust, and reinforce resilience. A strong crisis management model, built on real-time forensics, rapid containment, regulatory coordination, and transparent communication, ensures stability in the face of disruption.

Prevention is key, but readiness is vital. A swift, effective response framework limits damage and accelerates recovery. Crisis simulations, stress tests, and post-incident reviews transform challenges into opportunities, strengthening financial crime defenses for the future.

AUTHORS

Bhavin Shah, *Managing Director*
bshah@secretariat-intl.com

Bhavin has more than 20 years' experience helping clients navigate intricate legal matters, conduct multi-jurisdictional investigations, steer regulatory negotiations, manage crises, and implement robust anti-money laundering strategies.

Ralph Stobwasser, *Managing Director*
rstobwasser@secretariat-intl.com

Ralph is an expert in forensic investigations, anti-money laundering, combating the financing of terrorism, sanctions, business intelligence, and asset tracing with 20 years of experience working on engagements in the Middle East and around the world. He is a Certified Fraud Examiner and Certified Anti-Money Laundering Specialist.

Bryan Stirewalt, *Senior Advisor*
bstirewalt@secretariat-intl.com

Bryan is a globally recognized expert in financial crime, corporate governance, public policy, enforcement, and financial supervision. He has significant experience advising governments, financial regulators, and multinational corporations on complex regulatory challenges, financial crime compliance, and crisis management.

May Mhanna, *Managing Director*
mmhanna@secretariat-intl.com

May brings more than 17 years of experience in advising clients in financial and operational engagements. Her experience draws from working with a variety of clients, including governmental bodies and national and multinational enterprises within the financial services and public sectors.

Pooja Shah, *Associate Director*
pshah@secretariat-intl.com

Pooja is a Chartered Accountant with more than 10 years of expertise in financial investigations, regulatory compliance, and addressing bribery and corruption concerns.

Anmol Chandwani, *Senior Associate*
achandwani@secretariat-intl.com

Anmol is a Chartered Accountant and has close to seven years of experience in financial and corporate investigations, forensic accounting, anti-bribery and anti-corruption reviews, due diligences, and asset tracing across various industries.

Shivna Bhatia, *Associate*
shbhatia@secretariat-intl.com

Shivna has experience in risk management, financial statement analysis, regulatory investigations, business intelligence across various industries for investigative and compliance initiatives.

Sarah Morgan, *Marketing Manager*
smorgan@secretariat-intl.com

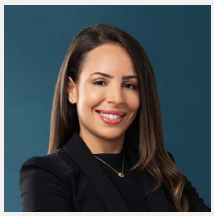
Sarah is a graphic designer and marketing professional with over 10 years of experience in design, digital marketing, and brand management.

OUR GLOBAL EXPERTS

Marcel Etschenberg
Munich, Germany
metschenberg@secretariat-intl.com

Greg Hallahan
Hong Kong, SAR
ghallahan@secretariat-intl.com

Norman Harrison
Washington DC, United States
nharrison@secretariat-intl.com



May Mhanna
Dubai, United Arab Emirates
mmhanna@secretariat-intl.com

Stephen Millington
Dubai, United Arab Emirates
smillington@secretariat-intl.com

Eric Poer
San Francisco, United States
epoer@secretariat-intl.com

Bhavin Shah
Dubai, United Arab Emirates
bshah@secretariat-intl.com

Brian Stapleton
London, United Kingdom
bstapleton@secretariat-intl.com

Ralph Stobwasser
Dubai, United Arab Emirates
rstobwasser@secretariat-intl.com

Bryan Stirewalt
Dubai, United Arab Emirates
bstirewalt@secretariat-intl.com

Charlie Warren
Singapore
cwarren@secretariat-intl.com

Ed Westerman
San Francisco, United States
ewesterman@secretariat-intl.com

SECRETARIAT EXPERTS ARE TRUSTED in the highest-stakes legal, risk, and regulatory matters around the world. Renowned law firms, leading corporations, and respected governmental entities turn to our disputes, investigations, economic, and data advisory services when the stakes are high. Quality, integrity, and independence are woven into every aspect of our work.

We would like to hear from you

info@secretariat-intl.com

secretariat-intl.com

Secretariat

secretariat-intl.com