Research report by Finextra Research,
in association with Eastnets

September 2024

eastnets

BROKEN INSIDE, BROKEN OUTSIDE: THE GLOBAL FIGHT AGAINST TRADE-BASED FINANCIAL CRIME

Uncovering the internal weaknesses and external pressures fuelling a $1.6 trillion challenge

Finextra

01 Foreword

Hazem Mulhim,
Founder and CEO
Eastnets

Silent saboteur: Unmasking the hidden threat of Trade-Based Financial Crime

Trade-Based Financial Crime (TBFC) is a global issue, draining $1.6 trillion annually from economies—funds that could otherwise fuel development, build infrastructure, and stabilise financial systems. Instead, these resources are diverted into criminal networks that operate across borders, exploiting the very institutions meant to protect global finance. This is a crisis that goes beyond numbers; it strikes at the core of trust and stability in the financial world.

Regulatory complexity compounds the issue. Institutions are overwhelmed by a maze of ever-changing regulations across multiple regions, struggling to maintain compliance while staying ahead of sophisticated criminal networks. But this isn't a challenge we can afford to shy away from—it's one we must confront head-on.

This is the long view we must take: the rise of AI and automation isn't something to fear. It's a solution to embrace. The institutions that adopt these technologies will not only protect themselves from financial crime, but they will also position themselves as leaders in a new era of finance. Technology can unify fragmented systems, bring together disconnected data, and create a stronger, more resilient foundation for the future.

Global cooperation is key. TBFC is not a challenge that any one institution or nation can tackle alone. Criminals don't respect borders, and our defences must be just as seamless. Financial institutions, regulators, and governments need to collaborate, share intelligence, and build a network that's as interconnected as the financial system itself.

The time for action is now. Technology offers us a path forward, but we must act swiftly. Institutions that fail to adapt will fall behind, facing mounting risks and regulatory scrutiny. But those that embrace AI and automation will lead the way, securing their place in the future of global finance.

The message is clear: evolve, innovate, and work together. That's the way forward.

02 Methodology

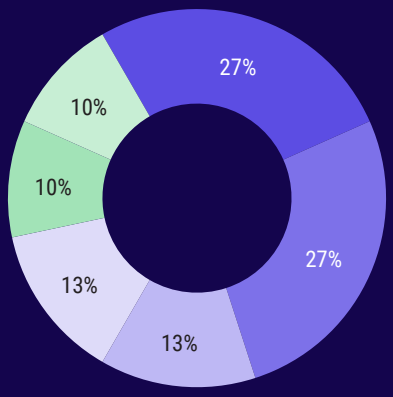
In the summer of 2024, a global survey revealed the alarming extent to which financial institutions remain unprepared in the face of the growing threat of Trade-Based Financial Crime (TBFC). The survey, encompassing 150 institutions from across the world, sheds light on the significant challenges, technology gaps, and fragmented risk management strategies that continue to enable TBFC.

Scope and participation

The survey included responses from 150 financial institutions representing key global financial centres:

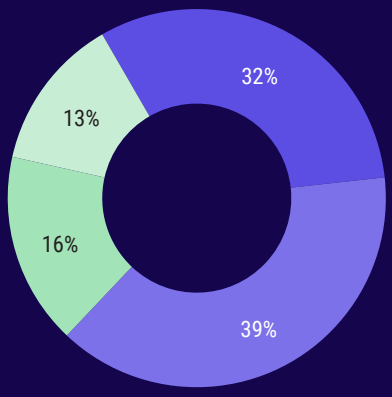
Of the respondents, 34% were C-level executives, with the remainder occupying senior management and director-level roles. This seniority ensures the insights represent both strategic oversight and operational realities.

Region



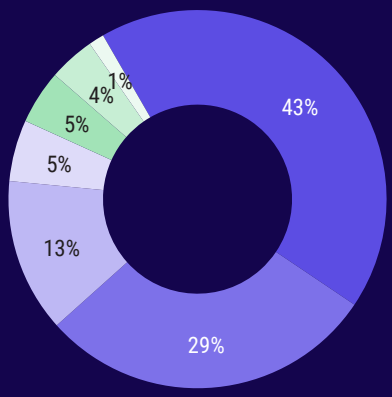
- Europe (including UK)
- North America
- Latin America
- Asia Pacific
- Middle East
- Africa

Organisational Size



- Large global banks (Tier 1) >$250bn
- International and national banks (Tier 2) $250 - $50bn
- Smaller national and regional banks (Tier 3) $50 - $10bn
- Banks (Tier 4) $10-1bn

Business Function



- Wholesale banking
- Corporate investment banking
- Transaction banking
- Structured trade finance
- Other (please specify)
- Treasury operations
- None of the above

Key data and analysis

The survey combined quantitative and qualitative data through self-administered questionnaires, with expert commentary from ING and ITFA, adding depth to the findings. The results highlighted critical weaknesses in TBFC risk management, particularly the vulnerabilities being exploited by increasingly sophisticated criminal networks.

03
Executive summary

Trade-Based Financial Crime: The $1.6 trillion blind spot

Trade-Based Financial Crime drains $1.6 trillion annually from the global economy—an amount comparable to the GDP of Australia. Financial institutions are struggling to keep up with increasingly sophisticated criminal networks that exploit gaps in global trade, creating a significant blind spot in risk management.

Key findings from the global survey of 150 financial institutions highlight critical challenges:

- **Institutional fragmentation**: 42% of institutions cite siloed data and disconnected workflows as major obstacles, with European banks facing the greatest difficulties (59%). It also exposed how TBFC risk management is typically distributed across three to four departments within most institutions. This fragmented structure creates significant gaps that criminal actors are exploiting.

- **Regulatory complexity**: 65% institutions identified regulatory complexity as a primary challenge. Institutions in Europe (68%) and North America (73%) are particularly burdened by evolving regulations, leaving them vulnerable to emerging financial crime techniques.

- **Inconsistent technology adoption**: Despite 87% of institutions recognising AI as essential for TBFC detection, the effective implementation of these technologies remains questionable when faced with fragmentation, data siloes and external challenges.

To tackle TBFC effectively, financial institutions must break down internal silos, centralise data systems, and prioritise the adoption of AI-driven tools. Without decisive action, they risk falling behind in the fight against financial crime and facing severe regulatory and reputational consequences.

Expert insights

Input from leaders at ING and ITFA reinforces the critical role of technology in combating TBFC, while also acknowledging the operational challenges that remain. Implementing AI-driven solutions at scale is proving to be a significant obstacle for many institutions, with the timeline for action growing ever tighter.

Global impact

The survey paints a clear picture of TBFC risk management practices across regions and institutional sizes, ranging from local banks to global financial giants. Striking differences emerged: European banks are struggling with data silos, while their North American counterparts grapple with regulatory overload. Yet, a common theme runs throughout: the urgency to act.

TBFC represents a looming threat, and financial institutions that fail to immediately invest in advanced technologies will face severe consequences. Conversely, those that embrace AI and automation will not only lead the future of financial security but will also solidify their position ahead of competitors scrambling to keep pace.

04

Trade-Based Financial Crime: A growing global crisis

Global trade drives the world economy, but beneath its surface, a shadow lurks. TBFC isn't just a small-time fraud operation—it's a sprawling network of illicit schemes that siphons billions from legitimate channels, leaving real-world devastation in its wake.

Consider that between 2008 and 2017, the global value gap (the discrepancy between perceived and actual value in imports and exports) reached $8.7 trillion, equivalent to the size of a G7 economy. Or that in 2023 alone, over **$1.1 trillion in illicit funds** flowed through financial systems across the Americas, and over **$951 billion in Europe**.

You might consider that according to a UN estimate, money laundering accounts for 2-5% of global GDP, or **$800 billion to $2 trillion annually**. Of that, **$240 billion to $600 billion** is linked to Trade-Based Money Laundering (TBML). Perhaps that in 2019, only 0.2% of money laundering reports submitted were related to TBML, despite it accounting for about 30% of all money laundering crimes.

But this doesn't do it justice. Instead, imagine a lower income economy on the African continent. In theory, revenue from trade should be funding schools, roads, and hospitals. But **$88.6 billion**, intended for development, vanishes each year due to TBFC. Children walk miles to underfunded schools, hospitals lack basic supplies, and the promise of growth remains a distant dream—all while criminal networks profit from the very trade meant to uplift these regions.

Criminals exploit every loophole available—falsifying trade documents, manipulating the value of goods, and using jurisdictional gaps to move dirty money. Across the Americas, $1.1 trillion of illicit funds flowed through financial systems last year, directly contributing to economic instability in countries already struggling with poverty and corruption. Families across the region face rising food prices and job losses as money is siphoned away, making recovery even harder for communities that need stability more than ever.

The fight against TBFC: A historical perspective

The roots of today's battle against financial crime trace back to 1989 when the OECD established the Financial Action Task Force (FATF) to address the unchecked flow of illicit funds through offshore financial centres. This led to a sharp increase in Anti-Money Laundering (AML) measures, requiring banks to follow strict Know Your Customer (KYC) protocols. Over time, a clean FATF record became a key credential for any institution looking to engage in serious global trade.

As the world moved towards digitisation, the FATF's initial focus on cash transactions expanded to encompass global trade, which introduced new avenues for the flow of illicit capital.

The technological fightback

Now, the same digitisation that has enabled new methods for TBFC also holds the key to fighting it. Advanced technologies, particularly artificial intelligence (AI) and machine learning (ML), offer financial institutions the ability to keep pace with the growing sophistication of criminal networks.

AI-driven systems can sift through mountains of data in real time, identifying suspicious patterns that human analysts simply cannot. From trade flows to pricing anomalies, machine learning algorithms are critical for spotting the warning signs of TBFC schemes. Generative AI, meanwhile, is becoming a game-changer in predictive risk assessment, helping institutions anticipate risks before they emerge.

Yet many organisations, especially in the Tier 2 or below range, struggle with fragmented systems and siloed data, which weakens their ability to detect and prevent TBFC. While Tier 1 banks can flex their muscle when it comes to people, resources and money, smaller banks don't have that ability. They don't see as much risk in terms of their exposure, because they're still doing things in disparate systems without creating a centralised view.

The wide range of Trade-Based Money Laundering typologies also presents a significant challenge to financial institutions. TBML schemes often involve multiple jurisdictions, numerous parties, and an intricate web of trade documents, making them difficult to detect without the right technology and data interoperability.

A critical crossroads

As a result of this, TBFC is not a problem that will fade away. It is deeply entrenched and growing more complex as global trade evolves. Institutions and regulators stand at a crossroads, with the tools to combat TBFC at their fingertips—if they choose to act. The cost of inaction is devastating; failure to adopt advanced technologies and break away from outdated processes will leave institutions floundering in a sea of risk.

As André Casterman, board member of the ITFA, points out: "Technology in the hands of criminals creates new operational challenges for institutions, for example in form of the volume of false positive cases. Institutions require more technology such as AI to further automate decision making in financial crime compliance. Technologies like generative AI need to be increasingly adopted to address initial use cases, like false positive cases, and later additional use cases, like credit decisioning."

This is not a fight that can be won with yesterday's methods. Institutions must embrace AI, break down internal silos, and work together globally. Only through coordinated, technology-driven action can they hope to stem the tide of TBFC and protect the integrity of the global economy.

The question is no longer if institutions will adopt these technologies, but how fast they can get there.

Sean Edwards, chairman of the ITFA, highlights: "Technology is the biggest factor in detecting TBFC once risk appetite has been taken into account, but there is a technology arms-race that is not, currently, being won by the banks and good actors. AI, for example, is being used better by the criminals than the victims."

05

Broken on the inside: What internal roadblocks are institutions facing?

Trade-Based Financial Crime thrives on complexity, and nowhere is that complexity more evident than within the financial institutions responsible for preventing it. These organisations often suffer from internal fragmentation—dividing responsibilities for TBFC risk management across multiple departments. This not only creates inefficiencies but also opens dangerous gaps that criminal networks exploit with increasing sophistication.

At the heart of this issue is the existence of organisational silos, where departments like compliance, fraud prevention, and trade finance operate independently, without consistent communication or data sharing. This isolation leads to a fragmented approach to risk management, which in turn creates severe consequences. Without coordination, different teams handle various aspects of TBFC risk, but no one department has a complete view of the institution's vulnerabilities. The result is a patchwork of oversight, where critical information remains trapped within disconnected systems, preventing institutions from seeing the bigger picture.

These gaps are compounded by the complexity of TBFC transactions, which often involve multiple parties, extensive documentation, and lengthy timelines. Navigating these challenges becomes even more difficult in institutions where internal systems are fragmented, with different departments managing parts of a transaction in isolation. This lack of a unified approach makes it nearly impossible to gain a clear, comprehensive view of the risks involved.

The extent of internal fragmentation

Survey data highlights the scale of the problem. Most financial institutions split TBFC risk management across three to four departments. On paper, this division might seem practical—after all, compliance, fraud, and trade finance are each involved in combating financial crime. However, without strong interdepartmental coordination, this structure leads to critical oversight gaps. Each department collects and manages its own data, often using separate systems that are not integrated or compatible. As a result, **data silos** form, where information that could expose criminal activity is trapped in disconnected systems.

3-4 departments

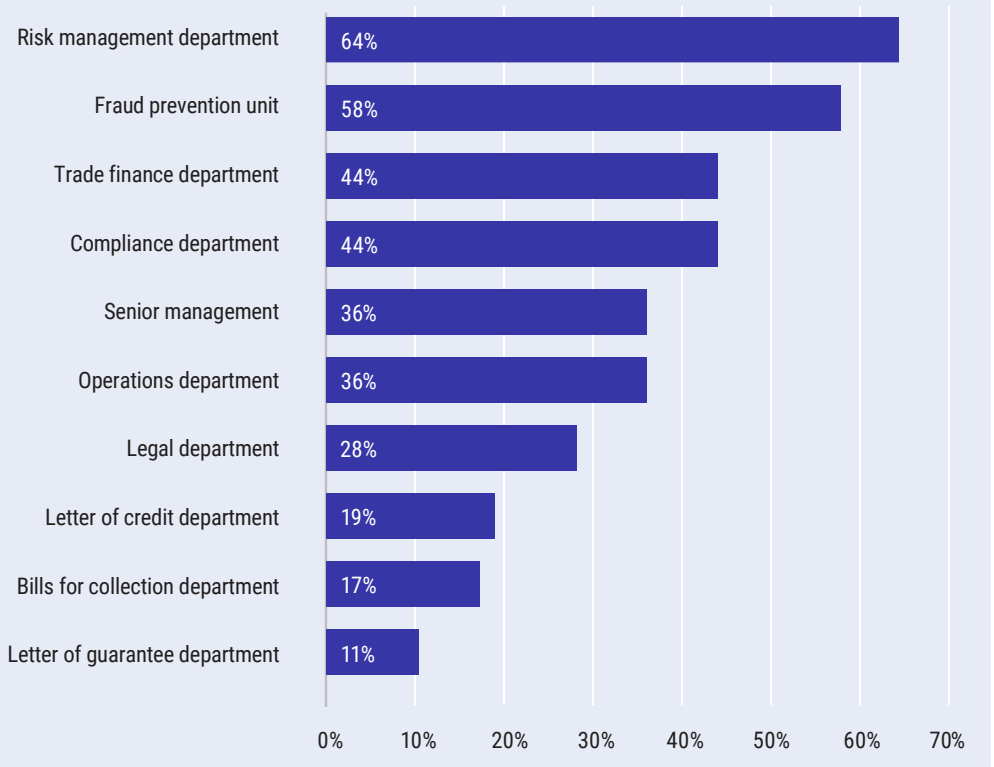
On average, between three and four departments are responsible for Trade-Based Financial Crime and associated risk in a single institution

These silos are not merely technical hurdles—they represent a fundamental breakdown in how institutions handle TBFC risks. For example, compliance teams may flag suspicious activity in trade transactions, but without access to trade finance data, they cannot fully assess the context or risk level.

Similarly, the fraud prevention team may detect unusual patterns, but without collaboration with the compliance or trade finance departments, those findings remain isolated. This fragmented workflow creates a reactive rather than proactive posture, where institutions are perpetually playing catch-up as criminal networks exploit the cracks in their defences.

GLOBAL RESPONSE

Where in your organisation does TBFC and associated risk sit?



The cost of siloed data and disconnected workflows

The consequences of these internal divisions extend far beyond inefficiency. Criminal networks are increasingly coordinated, leveraging global trade complexities to move illicit funds, evade taxes, and finance illegal activities. Meanwhile, the institutions tasked with preventing these schemes are fragmented, slow to respond, and often unaware of the full scale of the threat. TBFC schemes, by nature, involve multiple jurisdictions, layers of trade documentation, and seemingly legitimate transactions. Without a unified approach, financial institutions simply cannot keep up.

The **survey data** speaks volumes. Globally, **42% of respondents** cited siloed data and disconnected workflows as significant challenges in addressing TBFC. This number spikes in regions with complex regulatory landscapes. In Europe, for instance, **59% of respondents** reported that fragmented data systems were impeding their ability to combat TBFC. Even in North America, where open banking and data sharing is unregulated, **28%** still identified internal fragmentation as a major hurdle.

42% of respondents **globally** see siloed data and disconnected workflows as a challenge

28% of **North American** respondents see siloed data as a challenge

59% of **European** respondents see siloed data as a challenge

This fragmentation creates a kind of institutional blindness. The data needed to detect TBFC is often available, but it's scattered across multiple systems, preventing institutions from forming a comprehensive, real-time view of their risks. Criminals are adept at exploiting these blind spots, slipping through unnoticed as different departments within the same institution fail to connect the dots. Without a centralised risk management approach, institutions remain reactive, responding to threats only after the damage has been done.

The lack of ownership and accountability

One of the most insidious effects of this internal fragmentation is the absence of clear ownership over TBFC risk management. When responsibilities are spread across multiple departments, no single team or leader is accountable for overseeing the institution's defence against TBFC. This lack of accountability leads to **confusion, delayed decision-making**, and **slow responses to emerging threats**. Instead of having a centralised authority to coordinate efforts, institutions find themselves tangled in overlapping duties, inconsistent strategies, and poor communication.

Criminal networks are constantly evolving, refining their methods to evade detection. Meanwhile, institutions are bogged down by **bureaucratic inertia**—slow to adapt to new threats and hampered by internal disorganisation. In such an environment, it is not surprising that financial institutions are often one step behind the criminals they are trying to stop. Without a unified approach, they are left scrambling to respond to attacks after the fact, allowing criminals to slip through the cracks and continue their operations undetected.

The technology paradox

The introduction of advanced technologies, particularly AI and machine learning, have the potential to revolutionise the fight against TBFC. AI can process vast amounts of data in real time, identify suspicious patterns, and automate tedious manual processes like document verification. Yet even the most advanced technology will fail if deployed in a fragmented system. As Casterman observes, the sheer number of regulations impacting banks and the complexity of integrating multiple financial crime solutions make it difficult for institutions to keep up. Without **systemic coordination**, even the best technology cannot fulfil its potential.

Rob Kuiper, global head of SPS within transaction monitoring at ING, emphasises: "Technology and especially advanced analytics and AI play a crucial role in detecting TBFC. It enables financial institutions to increase the efficiency and effectiveness of mitigating risks related to TBFC. But it is also important to maintain a balance between automation and human expertise. Reliance on legacy systems, integration difficulties and cost constraints are some of the challenges that many organisations are facing."

Breaking the cycle: The path to unification

To effectively combat TBFC, financial institutions must undergo a fundamental transformation in how they approach risk management. The **first step** is to **dismantle the internal barriers** that isolate critical data and impede collaboration. Institutions need to **centralise their risk management systems**, ensuring that data from compliance, fraud prevention, trade finance, and other departments is accessible and integrated in real time. This unified approach will provide a comprehensive view of the institution's risk exposure, allowing for faster, more effective decision-making.

Next, institutions must establish **clear lines of accountability**. One team or leader should be responsible for overseeing TBFC risk management across the entire organisation. This ensures that responses to threats are coordinated, and that there is a consistent strategy in place to prevent criminals from exploiting gaps in the system.

Finally, institutions must **invest in training** their staff to fully leverage machine learning tools. Technology alone will not solve the problem—it must be implemented and managed by skilled professionals who understand both the capabilities and limitations of these systems. A well-trained workforce, supported by a unified risk management infrastructure, is essential to staying ahead of the constantly evolving threats posed by TBFC.

06

Broken on the outside: Regulatory frameworks and their global impact

If internal fragmentation within financial institutions is one half of the problem, the **regulatory maze** they face externally is the other. The battle against Trade-Based Financial Crime isn't only hampered by disjointed internal systems; it is compounded by a **complex and constantly shifting regulatory landscape**. Nowhere is this clearer than in the evolving trade sanctions frameworks that financial institutions must navigate, with the leading example being the UK's **Office of Trade Sanctions Implementation (OTSI)** poised to become one of the most formidable examples of this growing regulatory burden.

The regulatory labyrinth

For financial institutions, keeping pace with changing regulations is a near-impossible task. Global trade is inherently complex, and the regulations that govern it are often **inconsistent, overlapping**, and **ever-changing**. The UK's new trade sanctions framework, set to launch under OTSI in October 2024, represents a **new era of regulatory oversight**—one that will have far-reaching implications for institutions not just in the UK, but globally.

Under the new framework, **strict liability** rules will apply, meaning that institutions can face **severe penalties**—up to £1 million or 50% of the breach value—simply for failing to comply with trade sanctions, regardless of intent. This leaves no room for error. Financial institutions must ensure that they are fully compliant with sanctions, or risk not only crippling financial penalties but also reputational damage that can be difficult, if not impossible, to recover from.

OTSI's regime is designed to be unforgiving. Financial institutions will no longer be able to rely on plausible deniability or good faith efforts to comply. The expectation is absolute adherence, and the stakes are incredibly high. While this framework represents a necessary tightening of the rules to combat financial crime, it also creates a **compliance nightmare** for institutions already grappling with internal inefficiencies and fragmented systems.

Global disparities and regional complexities

The UK's new trade sanctions framework is just one part of a broader **global patchwork of regulations** that institutions must navigate.

Casterman highlights: "The main challenges are the number of regulations impacting banks and how they evolve, the plethora of technology solutions in the area of financial crime compliance and the operational complexity when implementing multiple solutions."

The situation becomes even more complicated when viewed on a global scale. Financial institutions operating across multiple jurisdictions must comply with not just one regulatory regime but dozens, each with its own set of rules, interpretations, and enforcement mechanisms. In Europe, for example, **65% of survey respondents** cited regulatory complexity as their most pressing concern in managing TBFC risks.

This patchwork creates significant **disparities in enforcement**. In regions like Africa, where regulatory frameworks are less stringent, financial institutions may find themselves inadvertently non-compliant when engaging in global trade. In fact, only **38% of African respondents** cited regulatory challenges as a significant concern—suggesting a lack of stringent enforcement, which in turn provides opportunities for criminal networks to exploit.

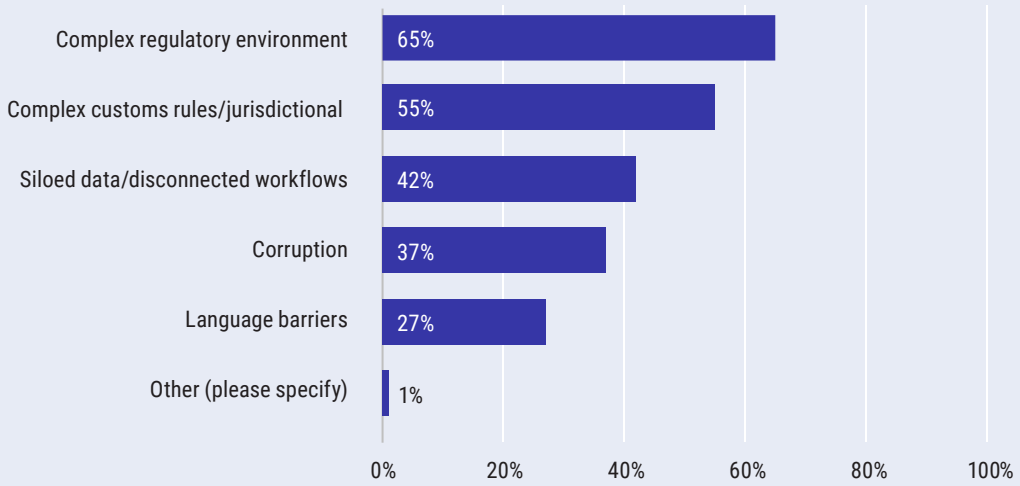
Criminals know this all too well. **Sophisticated TBFC networks** exploit these regional disparities, moving illicit funds through jurisdictions with weaker enforcement, allowing them to evade detection. This regulatory unevenness creates **vulnerabilities in the global financial system**, which criminals use to their advantage. The problem, then, is not just the volume of regulations but the **inconsistency of their application** across regions.

The burden of compliance

For financial institutions, the sheer volume of rules they must follow can feel insurmountable. Each market, each region, and sometimes each individual institution faces its own specific set of requirements. As new frameworks like OTSI or the United Arab Emirates' new AML act come into play, institutions are forced to **divert enormous resources** towards compliance—resources that could otherwise be focused on detecting and preventing TBFC.

GLOBAL RESPONSE

What challenges around Trade-Based Financial Crime is your institution currently facing?



Survey data underscores this reality. **65% of institutions globally** identify regulatory complexity as one of their biggest challenges in managing TBFC risks. And it's not just about the number of regulations—it's the pace at which they change. Rules that were compliant last year may no longer be sufficient today, creating a constant game of catch-up for financial institutions. Worse still, this constant churn often leaves institutions more focused on **managing bureaucracy** than addressing the actual risks posed by TBFC.

Kuiper mentions that one of the biggest risks is that "TBFC schemes are evolving and getting more and more sophisticated. This requires financial institutions to constantly adapt and invest to keep up with the latest developments. Regional differences are exploited because of different levels of regulatory oversight and enforcement capabilities, resulting in higher TBFC risks in regions with less stringent regulations."

Technology: A lifeline amidst regulatory challenges

In the face of this regulatory chaos, **technology offers a lifeline**. AI and automation can streamline compliance processes, allowing institutions to stay on top of constantly shifting regulations. By integrating AI-driven compliance solutions, institutions can automate tasks like **transaction screenings, real-time anomaly detection**, and ensuring that **trade-related documentation** aligns with the most current regulatory standards. This not only reduces the risk of non-compliance but also frees up human resources to focus on more strategic tasks.

As criminals refine their methods, institutions recognise the need to evolve their defences. Looking ahead to 2025, 91% of respondents indicated plans to prioritise automation within their risk management strategies, underscoring the sector's recognition of AI's critical role. Furthermore, 85% see advanced AI and generative AI as essential tools for optimising processes and staying ahead of ever-shifting criminal tactics.

91%

Increasing automation is a priority for 91% of respondents in 2025.

85%

of respondents are focusing on advanced AI and generative AI implementation.

However, despite the clear benefits and the recognition of AI's impact, the effective implementation of these tools remains questionable. Unless internal and external challenges are addressed, and data siloes are eliminated, institutions remain more vulnerable than ever, particularly as criminals use increasingly sophisticated methods to evade detection.

The cost of inaction

Conversely, consequences of non-compliance are significant and growing. With new frameworks, financial institutions are under greater scrutiny than ever before. The cost of failing to comply with sanctions and other regulations is not just financial—**reputational damage** can be even more devastating. A single compliance failure can result in lost customers, damaged partnerships, and a tarnished reputation that could take years to rebuild.

And yet, for all the focus on regulations, the frameworks themselves are often **behind the curve**. While institutions wrestle with bureaucratic hurdles, **criminal networks continue to evolve**, always staying one step ahead. Regulatory bodies may introduce new rules and requirements, but these are often **reactive**, addressing yesterday's problems rather than anticipating tomorrow's challenges. This lag in regulatory enforcement creates a dangerous mismatch between criminal innovation and institutional compliance.

The future of regulation: Coordination and innovation

To move forward, there must be greater **coordination between regulators** and financial institutions. Simply piling on more rules is not the answer. What's needed is a smarter, more streamlined approach—one that leverages technology to automate compliance, reduces the burden on institutions, and ensures that regulations are applied consistently across jurisdictions.

Moreover, regulators must work more closely with institutions to anticipate new risks rather than merely reacting to existing ones. By fostering greater collaboration, both parties can stay ahead of criminal networks, rather than falling behind them.

In conclusion, while new regulatory frameworks represent a significant step forward in the fight against TBFC, it highlights broader challenges for financial institutions when navigating the morass of global regulations.

Compliance has become a burden—one that institutions cannot handle alone. Through better coordination, smarter regulation, and the adoption of advanced technologies, there is a path forward. But the cost of inaction is clear: those who fail to adapt will be left behind, vulnerable to both regulatory penalties and the ever-evolving tactics of criminal networks.

07 Recommendations

TBFC continues to pose a significant threat to global trade and financial institutions. To combat this evolving threat, institutions must adopt a more proactive, coordinated, and technology-driven approach to TBFC risk management. This chapter outlines key recommendations for building a robust defence against TBFC, breaking down internal barriers, and navigating the external regulatory landscape.

Practical integration of AI in TBFC risk management

The complexity and scale of TBFC present significant challenges for financial institutions, particularly when relying on manual systems and traditional analytics.

Machine learning and AI play a pivotal role in modernising TBFC risk management, helping financial institutions improve operational efficiency and enhance the detection of suspicious activities. Key practical applications include:

- **AI-driven transaction monitoring**: AI can analyse transaction patterns to detect anomalies such as over/under-invoicing and circular trading, streamlining the identification of potential TBFC risks.
- **Continuous sanctions and watchlist screening**: AI systems continuously screen trade transactions and documents against global sanctions lists, ensuring real-time updates and reducing non-compliance risks.
- **Dual-use goods detection**: AI improves accuracy in identifying high-risk goods by cross-referencing trade documents with curated lists, minimising false positives and enabling faster detection of illicit items.
- **Document digitisation and verification**: AI automates the extraction and verification of data from trade documents using technologies such as Optical Character Recognition (OCR) and Natural Language Processing (NLP), reducing manual errors and improving process efficiency.

- **Predictive risk modelling**: AI analyses historical trade data to predict emerging risks, allowing institutions to adjust strategies proactively and stay ahead of TBFC trends.

- **Vessel tracking and geolocation monitoring**: AI integrates vessel tracking with geolocation data to monitor movements in real time, screening for high-risk routes and detecting sanctions violations.

By incorporating AI into TBFC management, institutions can reduce operational risks, improve real-time detection capabilities, and maintain a proactive stance against the evolving threats of Trade-Based Financial Crime.

Building a winning TBFC risk management strategy

1. Centralise risk management: Break down internal silos

The first step in effectively combating TBFC is to **break down internal silos** that fragment responsibility across different departments. TBFC risk management is often distributed between compliance, fraud prevention, and trade finance, each operating in isolation. This fragmented structure creates blind spots that criminal networks exploit. To counter this:

- **Establish a unified risk management team**: Centralising TBFC oversight under a single team or leader ensures clear ownership of risk management responsibilities. This team should have full visibility into all aspects of TBFC risks, coordinating efforts across departments to prevent duplication of effort and oversight gaps.

- **Integrate data systems**: Fragmented systems are a major roadblock to detecting TBFC. Institutions should invest in creating an integrated platform where data from different departments can be accessed and analysed in real time. A centralised system eliminates data silos and provides a comprehensive view of risk exposure, allowing institutions to detect patterns of TBFC more effectively.

- **Develop cross-functional collaboration**: Encourage regular communication and collaboration between departments to ensure a holistic view of TBFC risk. Institutions should hold cross-functional meetings to discuss emerging threats, review suspicious activity, and coordinate responses in real time.

2. Leverage advanced technology: Embrace AI at scale

Technology, particularly AI and automation, is no longer a luxury but a necessity in the fight against TBFC. However, many institutions are still lagging in their adoption of these tools. To stay ahead of increasingly agile criminal networks, institutions must fully embrace AI and integrate it into every level of their risk management strategy. Here's how:

- **Implement AI-driven detection systems**: AI can process vast amounts of data in real time, identifying suspicious patterns and anomalies that human analysts might miss. Institutions should deploy machine learning algorithms to monitor trade flows, pricing discrepancies, and transaction behaviours that signal TBFC schemes. By reducing false positives, AI tools can also ensure that investigators focus their efforts on genuine risks.

- **Automate manual processes**: Institutions should use machine learning and automation to streamline labour-intensive processes like document verification, sanctions screening, and transaction monitoring. Automated systems can scan large volumes of trade documents, flagging discrepancies in invoices, bills of lading, and certificates of origin in real time. This reduces reliance on human-driven processes that are prone to error and inefficiency.

- **Invest in predictive analytics**: Generative AI and machine learning can be used to predict and assess risks before they materialise. Predictive models can analyse historical data to anticipate emerging trends in TBFC, allowing institutions to adjust their risk management strategies pre-emptively. Proactively identifying risks can reduce the chances of institutions being caught off guard by new criminal tactics.

- **See the bigger picture**: AI's value goes beyond reducing false positives. Financial institutions need to connect digital payments, documents, and vessel tracking to see the bigger picture. AI can spot patterns, like misinvoicing, across these data points, helping to close gaps that criminals can exploit.

3. Strengthen KYC and enhanced due diligence: Know your customer like never before

Criminal networks often exploit weaknesses in Know Your Customer (KYC) and Enhanced Due Diligence (EDD) processes to slip through the cracks. Institutions must move beyond traditional KYC methods and adopt AI-powered profiling to detect and mitigate risks before they escalate. Here's how institutions can strengthen their KYC and EDD processes:

- **Implement advanced KYC systems**: Use machine learning and data analytics to build enhanced customer profiles. AI can identify hidden relationships, shell companies, and high-risk individuals that traditional KYC methods might overlook. These enhanced profiles allow institutions to flag suspicious entities before onboarding them, preventing criminals from entering the financial system in the first place.

- **Adopt dynamic monitoring**: Risk profiles are not static. Institutions must use continuous monitoring systems to reassess customer risk throughout their lifecycle. AI-driven EDD systems can automatically update risk profiles as new data becomes available, ensuring that institutions stay ahead of evolving threats.

- **Utilise blockchain for transparency**: Blockchain technology can provide an immutable and transparent record of trade transactions, reducing the risk of manipulation. By using blockchain to verify trade documents and track the movement of goods, institutions can ensure greater transparency and accountability in international trade.

4. Prioritise compliance through technology: Navigate regulatory complexity

With regulations becoming increasingly stringent, financial institutions must prioritise compliance automation to avoid penalties and reputational damage. The evolving regulatory landscape requires a flexible, tech-driven approach to compliance. Here's what institutions should do:

- **Automate compliance workflows**: Use machine learning to automate compliance checks, including sanctions screening, document validation, and anomaly detection. ML tools can quickly adapt to changing regulatory requirements, ensuring that institutions remain compliant with the latest rules.

- **Integrate real-time monitoring**: Compliance should not be a once-a-year audit; it needs to be a continuous process. Institutions should implement real-time monitoring systems that track transactions and trade documents as they occur, allowing them to spot non-compliance before it becomes a costly breach.

- **Collaborate with regulators**: Institutions should engage with regulators proactively to stay informed about upcoming changes in trade sanctions and compliance requirements. Developing relationships with regulatory bodies can also facilitate smoother compliance reviews and audits.

5. Build a culture of collaboration: Break down external barriers

TBFC is a global problem, and no single institution can tackle it alone. Criminal networks operate across borders, taking advantage of **jurisdictional loopholes** and **regional disparities** in regulatory enforcement. To counter this, institutions must foster **collaborative partnerships** across the financial industry and beyond:

- **Establish cross-border partnerships**: Financial institutions should work closely with regulators, law enforcement agencies, customs officials, and industry peers to share intelligence and best practices. Criminal networks thrive on isolation and lack of coordination; by building a collaborative ecosystem, institutions can close the gaps that criminals exploit.

- **Create industry-wide information-sharing platforms**: Institutions should participate in industry initiatives that facilitate the sharing of real-time information on emerging TBFC threats. By pooling data on suspicious activity and trade transactions, institutions can build a collective defence against criminal networks.

- **Engage in joint investigations**: Institutions should consider partnering with regulators and law enforcement on joint investigations into large-scale TBFC networks. Criminals operate globally, and coordinated, multi-jurisdictional investigations are essential to dismantling their operations.

- **Form partnerships**: Institutions should work with organisations that have partnerships with regulatory bodies like the Basel Committee and central banks, and with industry peers to ensure a unified approach. By working together, institutions can improve their ability to detect and prevent financial crime, leveraging collective knowledge and resources to strengthen the integrity of the global financial system.

6. Equip and empower teams: Invest in human capital

While technology is crucial, it cannot replace the **expertise of well-trained professionals**. To fully leverage the power of AI and automation, financial institutions must invest in continuous training programmes that equip employees to interpret AI-generated alerts and make informed decisions based on those insights.

- **Train staff in AI and compliance**: Employees should receive ongoing training on the capabilities and limitations of AI-driven risk management tools. This training will enable them to make data-driven decisions and confidently act on AI-generated alerts.

- **Develop TBFC experts**: Institutions should foster in-house TBFC expertise by building specialised teams that focus on identifying and mitigating Trade-Based Financial Crime. These experts should stay abreast of the latest criminal tactics and regulatory developments to ensure the institution remains ahead of the curve.

7. Evolve with the threat: Adopt an agile, forward-looking approach

TBFC is not a static threat—it evolves constantly, as criminal networks refine their tactics to evade detection. Financial institutions must adopt an **agile approach** to risk management, continuously adapting to new threats and technologies:

- **Review and update strategies regularly**: Institutions should frequently reassess their TBFC risk management strategies, adjusting to new criminal tactics, regulatory changes, and technological advancements. A dynamic, flexible approach will keep them prepared for whatever the future holds.

- **Invest in research and development**: Staying ahead of criminals means staying ahead of technological trends. Institutions should dedicate resources to R&D, exploring new technologies such as quantum computing, blockchain, and AI innovations that can enhance their TBFC defences.

- **Foster a culture of innovation**: Encourage employees at all levels to contribute to the institution's evolving TBFC strategy. Innovation should be embedded in the institution's DNA, with a constant focus on improving systems, processes, and defences.

08 Conclusion

TBFC represents one of the greatest threats to the integrity of the global financial system. Each year, trillions of dollars are siphoned from legitimate channels, funding criminal networks, destabilising economies, and undermining the very foundations of governance and trade. TBFC is no longer an issue that institutions can afford to overlook or manage passively—**the stakes are simply too high**.

This report has uncovered the dual challenge institutions face: **internal fragmentation** and **external regulatory complexity**. Together, they create a perfect storm of vulnerability. Financial institutions, hamstrung by siloed data and disconnected workflows, are often ill-equipped to detect and prevent the increasingly sophisticated schemes used by criminal networks. On the outside, the regulatory landscape is growing more labyrinthine, making compliance not just a challenge but a burden, diverting resources away from fighting TBFC itself.

But amidst this morass, there is a path forward. **Technology is the key**, with ML, AI and automation offering unprecedented capabilities to detect, prevent, and mitigate TBFC risks. By integrating these tools, institutions can break down internal barriers, streamline compliance efforts, and focus on what truly matters—staying ahead of the criminal networks that threaten their very existence.

Yet technology alone will not solve the problem. It must be paired with **strong leadership, clear accountability**, and **collaborative partnerships** across the financial ecosystem. Institutions must centralise their risk management, foster a culture of innovation, and engage with regulators and peers to share intelligence and coordinate defences. This is not a battle any one institution can win alone—it requires a unified, global response.

The time for reactive measures is over. Institutions must act decisively, with urgency, and with a clear-eyed view of the risks they face. Criminal networks are evolving every day, exploiting any gaps they find. Institutions that fail to adapt, that remain mired in outdated processes and fragmented systems, will inevitably fall behind. The cost of inaction is not just financial—it's existential. Reputational damage, regulatory penalties, and operational collapse are the inevitable consequences for those who do not rise to meet this challenge.

But for those institutions willing to embrace change, the opportunity is immense. By harnessing the power of technology, fostering collaboration, and adopting a proactive approach, financial institutions can not only protect themselves from TBFC but also position themselves as leaders in the fight against global financial crime. The institutions that act now will define the future of financial security—they will be the ones that set the standard for the industry, not just in compliance but in resilience and innovation.

The turning point is here. The question is not whether institutions will face this challenge, but **how** they will respond. Those that adapt, evolve, and unite in the fight against TBFC will emerge stronger, more secure, and ready for the future. The path forward is clear—the time to act is now.

09
Glossary of key terms

1. **Trade-Based Financial Crime (TBFC)**: The use of international trade to disguise the movement of illicit funds. TBFC schemes often involve misinvoicing, over- or under-invoicing of goods, and manipulation of trade documents.
2. **Money Laundering**: The process of disguising the origins of illegally obtained money, typically by passing it through a complex sequence of banking transfers or commercial transactions.
3. **Trade-Based Money Laundering (TBML)**: A specific type of money laundering that uses trade transactions to move money across borders illicitly, often through falsified trade documents or misrepresented invoices.
4. **AI (Artificial Intelligence)**: A branch of computer science that involves creating systems capable of performing tasks that normally require human intelligence, such as problem-solving, pattern recognition, and decision making.
5. **Machine Learning (ML)**: A subset of AI that allows systems to learn and improve from experience without explicit programming. ML algorithms detect patterns and make decisions based on data.
6. **Generative AI**: A type of AI that can generate content, such as text, images, or even data, based on patterns learned from training data. In TBFC, it can be used for predictive risk assessments and anomaly detection.
7. **OCR (Optical Character Recognition)**: Technology that converts different types of documents, such as scanned paper documents, PDFs, or images captured by a digital camera, into editable and searchable data.
8. **NLP (Natural Language Processing)**: A branch of AI focused on the interaction between computers and humans through natural language. NLP is used to analyse text and automate document processing.
9. **Know Your Customer (KYC)**: A process used by financial institutions to verify the identity of their clients, ensuring they understand the client's financial activities and risk level.
10. **Customer Due Diligence (CDD)**: A component of KYC, CDD refers to the procedures that financial institutions use to collect and evaluate relevant information about a customer to assess potential risks of illegal financial activity.
11. **Enhanced Due Diligence (EDD)**: An advanced level of KYC that involves more thorough verification and monitoring for clients deemed high-risk, often required for transactions involving large sums or politically exposed persons (PEPs).

12. **Siloed Data**: Data that is isolated within a particular department or system, which leads to inefficiencies and fragmented workflows, making it difficult to access and analyse across an organisation.
13. **Fragmented Workflows**: Disconnected business processes that are spread across multiple departments or systems, often leading to inefficiencies and gaps in compliance or risk management.
14. S**anctions Screening**: The process of ensuring that a financial institution's transactions do not involve individuals, entities, or countries that are subject to international sanctions.
15. **Transaction Monitoring**: A system used by financial institutions to monitor customer transactions in real-time or retrospectively for suspicious activity, which could indicate money laundering or TBFC.
16. **False Positive**: In the context of compliance and risk management, a false positive occurs when a system flags a legitimate transaction or activity as suspicious or risky, requiring further investigation.
17. **Predictive Risk Management**: A proactive approach to risk management that uses data, AI, and analytics to anticipate and mitigate risks before they materialise, rather than reacting to them after the fact.
18. **Compliance Risk**: The risk of legal or regulatory sanctions, financial loss, or reputational damage due to failure to comply with laws, regulations, or internal policies.
19. **Office of Financial Sanctions Implementation (OFSI)**: A UK government body responsible for overseeing financial sanctions enforcement, established to strengthen oversight and penalties related to trade finance.
20. **Blockchain**: A decentralised, digital ledger used to record transactions across multiple computers securely. In TBFC, blockchain can be used for secure, transparent document verification and transaction tracking.

10 About

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers. The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information:
Visit **www.finextra.com** and become a member,
follow **@finextra** or reach us via **contact@finextra.com**.

Eastnets

Eastnets is a global provider of compliance and payment solutions for the financial services sector. Through our experience, expertise and technology we enable safe and secure participation in the global financial economy for over 800 financial institutions globally, including 15 of the top 50 banks, and 22 of the world's central banks.

For more than 40 years, we've worked to keep the world safe and secure from financial crime. We do this by helping our partners manage risk through Sanction Screening, Transaction Monitoring, analysis, and reporting, plus industry leading consultancy and customer support.

For more information:
Visit **www.eastnets.com**

Finextra Research Ltd
77 Shaftesbury Avenue
London,
W1D 5DU
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com