Trade Digitalisation Taskforce
Fraud prevention recommendations

ACT

AFB

BAFT

British Chambers of Commerce

BIFA®
BRITISH INTERNATIONAL FREIGHT ASSOCIATION

CHARTERED INSTITUTE OF EXPORT & INTERNATIONAL TRADE

fsb
Experts in Business

GLEIF

ICC United Kingdom

ITFA

UK FINANCE

Preventing fraud in cross-border trade

1

Fraud, in all its forms, acts as a drag on economic growth, increasing the cost of trade and diverting valuable resources that could otherwise be used more effectively to increase trade and deliver growth. Financial institutions (FIs) invest significant time and effort in managing the risk of fraud and the Taskforce has put together a high level summary of such efforts and recommendations and best practices for FIs more broadly (see Appendix 1 on page 7). The summary highlights some of the challenges and manual nature of controls and due diligence that would benefit from automation.

Digitalising trade and the smarter use of technology solutions presents a real opportunity to automate, improve efficiency and accuracy in a real time environment, to shut fraudsters out of trade. According to ICC research, doing so using a coordinated approach involving collaboration between government, regulators and industry could generate £25bn in new economic growth, free up £224bn in efficiency savings, and deliver real-world economic benefit to the UK economy and it's international trade partners.

The Economic Crime and Corporate Transparency Act (ECCTA) of 2023 introduced a new "failure to prevent fraud" offence in the UK. This aims to encourage organisations to take responsibility for poor systems and controls that could be exploited by individuals to break the law. The new offence makes an organisation liable if it fails to have reasonable fraud prevention procedures in place. It applies to large organisations in all sectors that meet two or more of the following criteria: more than 250 employees, more than £36 million turnover, and more than £18 million in assets. This is timely and similar to the Failure to Prevent Bribery & Corruption. The government is due to produce specific guidance providing organisations with information about what reasonable procedures will look like again similar to the UKBA.

The foundational solutions to fraud prevention are, at their core, the same as in other parts of the digital trade ecosystem and include effective regulatory cooperation with industry, more innovation, better quality of data and better sharing of data, use of standardised data, connectivity of technology systems and the adoption and use of Legal Entity Identifiers (LEIs). Government procurement and tax systems will also benefit from a unified approach across the public and private sectors.

This is about government and regulators helping enable FIs to establish leaner solutions that work for everyone in trade. Smarter use of technology and better cooperation and coordination will deliver better solutions that are interoperable and compatible across the entire trade ecosystem. Too often, no single entity appears responsible for convening actors across the public and private sectors to solve the fraud challenge. The joint Department for Business and Trade-Barclays-ICC United Kingdom's Trade Digitalisation Taskforce provides such a forum, bringing together stakeholders across the trade ecosystem to provide strategic advice to the UK government on advancing the digitisation agenda.

Recommendations

2

Listed below are four high-level recommendations that will deliver the solutions and align to other opportunities in making trade cheaper, faster, simpler and more sustainable and accessible to UK businesses. The recommendations and solutions are aimed at UK level decision makers and aligned with solutions at international level.

1 Deeper regulatory cooperation with industry to promote innovation

We recommend that key representatives from the Financial Conduct Authority (FCA), the Central Digital and Data Office (CDDO) and The Alan Turing Institute (The Turing) join the Trade Digitalisation Taskforce to agree practical actions that can be taken to foster more innovation and smarter technology-based solutions to prevent fraud.

Banks, in their effort to prevent fraud, would benefit considerably from greater engagement and support from our financial regulators, government and national institutes to both promote greater data sharing and more innovative technology solutions in fraud identification and prevention systems. Today, this collaborative and innovative environment doesn't exist for the prevention of fraud in cross-border trade finance and makes it harder for UK companies to compete in this space.

In addition, we would benefit from greater regulatory guidance around addressing fraud risk. Specifically, prevalent regulation around anonymous or opaque corporate structures must be strengthened such that FIs are able to positively match beneficial owners and key controllers within a wider pool of entity level information that is publicly available (for instance through Companies House).

2 Standardising information and connecting government and financial systems

We would welcome specific engagement with the National Economic Crime Centre (NECC)'s JMLIT partnership to identify a practical solution that can be quickly adopted to better identify fraudsters in the system and to report back to the Trade Digitalisation Taskforce with suggested next steps.

Both government and FIs share a common ambition to shut fraudsters out of trade and both have access to unique intelligence and insight on fraudsters in the system. However, basic supporting infrastructure such as Application Programming Interface (API) based alert systems between NECC agencies and FIs are not in place to help identify fraudsters quickly and remove them from FI systems. For example, fraudster name lists sourced from agencies involved in the NECC's JMLIT partnership (e.g., City of London Police (CoLP), HMRC, Serious Fraud Office (SFO) and National Crime Agency [NCA]) can be considered as part of this practical solution.

The UK's private sector has been systematically fostering APIs for several years now. API can integrate directly into an organisation's systems and provide a secure channel to seamlessly transmit pre-authorised data fields to another organisation in real time whenever triggered or requested. Such solutions are neither complex, nor expensive but would help leverage the collective knowledge and data available between government and industry.

To support large scale adoption of API connections to the industry, and to further enhance public / private Sector collaboration, the UK's Central Digital and Data Office (CDDO) has recently created a central API Catalogue for all UK public sector organisations. We recommend API connectivity becomes mandated by relevant public sector organisations requiring industry to develop channels for exchanging identifying information about fraudsters across their networks.

Given recent advancements in data science and Artificial Intelligence (AI) research, this practical solution could potentially benefit from a challenge led approach in collaboration with The Alan Turing Institute, recently tasked with delivering the UK's AI strategy, including areas such as national security.

3 The role of Companies House

We recommend that the Government Procurement Service lead by example and mandate the use of Legal Entity Identifiers for all government suppliers.

Companies House (CH) plays a critical role in the provision of accurate information on entities within the system. New objectives and measures recently announced by the UK Registrar of Companies are welcomed by the industry. In particular, the new measure to introduce identity verification for all new and existing registered company directors, people with significant control, and those who file on behalf of companies is seen as a key development by FIs seeking to fulfil their KYC obligations using this information.

The current review of CH is welcome but not enough in itself unless aligned to the international common identity framework provided by the Global Legal Entity Identifier Foundation. National solutions do not provide an identity solution in a cross-border environment where an international, interoperable framework is required.

The LEI data pool can be regarded as a global directory, which greatly enhances transparency across businesses globally.

Driving accuracy of both client and financial data, as a result promotes market integrity while containing financial fraud. Adding LEI's into CH can provide wider benefits:

- Clear and unique identification of legal entities in financial transactions.
- Enhanced ability for FI's to evaluate risk.
- Improved data reconciliation across borders.
- Provides details about an entity's ownership structure.
- Linkage to credit reference agencies.

4 The role of public procurement

Government is a major influencer in the way we do business and trade. As a buyer and seller of goods and services in its own right, it is also exposed to fraud risk in the same way as all other companies and FIs . Government, should therefore, lead by example in applying the solutions set out in this paper to its own public procurement systems.

Appendices

3

Appendix 1: Summary of fraud risk best practices and processes for financial institutions

1 Introduction and background

The misuse of Trade Finance for fraudulent purposes or first party lending fraud is found primarily between two related risks: first, the provision of falsified financial information that results in an entity being approved for a trade loan they do not qualify for (financial misrepresentation) and second, the risk of collusion between both related or unrelated parties.

The United Kingdom's 'Shutting fraudsters out of trade' report1 highlights that the banking industry spends billions each year fighting fraud, but criminals continue to commit this crime. In a US$5tn global trade financing market, the report suggests it is reasonable to estimate that 1% of the total trade finance transactions — or US$50bn — are susceptible to various types of fraud.

The complexity of trade transactions and the role played by FIs engaging in trade finance, especially inherent in the physical documentary nature of trade transactions, makes it difficult for FIs to verify the accuracy of the trade transactions and information. This makes it consequently easier for fraudulent activity to go undetected.

2 Objectives

This summary provides an updated view on the ongoing challenges associated with the implementation of controls relating to the detection and prevention of trade fraud; the most common financial industry-wide approaches to managing fraud risk; and the effectiveness of potential fraud controls.

It also aims to summarise best practices and recommendations for FIs engaged in or looking to start or engage more in trade finance, recognising that a variety of approaches exist, based on the individual circumstances of respective institutions, and that no single solution or approach will be appropriate for all.

3 Scope

This summary limits itself to a discussion specific to the plausibility of implementing fraud controls for trade finance, rather than the much broader topic of Trade Based Financial Crime (TBFC), where it may be noted that FIs, in offering a wide range of banking products (including trade finance products) would no doubt be party to payment flows which offer significantly less information than a typical trade finance transaction.

[1] Shutting fraudsters out of trade – Sustainable trade through digital empowerment (c4dti.co.uk)

4 Regulatory requirements

FIs have a strong incentive to protect themselves from fraud. The Financial Crime Guide (FCG) published by the Financial Conduct Authority (FCA) outlines certain prevalent fraud themes accompanied by a basic walkthrough of good and bad practices.[2] This guidance looks at fraud as being financial crime and therefore attracting attention as part of the risk-based approach undertaken by FIs towards combatting financial crime more broadly. We would warmly welcome closer cooperation with the FCA and other relevant parties, to discuss the 4 recommendations made in this paper and align on next steps going forward.

5 Ongoing challenges associated with fraud prevention

5.1 Lack of transparency in corporate ownership reference points

Anonymous or opaque corporate structures prevent FIs from forming a complete ownership pattern across clients and counterparties, thereby increasing the risk of collusion resulting in fraud.

5.2 Legitimate reasons supporting most fraud risk typologies

Several influencing factors dictate why genuine payments may match to known fraud risk typologies and this results in huge overheads in attempting to detect fraud.

5.3 Transaction complexity

As outlined earlier, cross-border transactions and certain structured trade solutions can be inherently more complex in nature; the additional and more challenging controls applied to managing these risks can be unwieldy and risk increasing costs in the trade and impacting processing speed of genuine trade flows.

5.4 The role of FIs engaged in trade finance and documentary risk

FIs relate with the risk associated with a transaction, i.e. the risk evident to the transaction documents which may not evidence risk indicators related to certain known documentary fraud typologies. Hence, FIs have a better chance of detecting fraud if their corporate client's activity is assessed holistically (and not just on a paper trade transaction basis) also taking into consideration the credit risk.

6 Current approaches to fraud detection and prevention

6.1 Manual review/escalation by processing staff

The most common industry approaches to combatting fraud risk continue to place most reliance on the human element, i.e., a subjective judgmental call taken by transaction processing staff to determine if the physical trade documents themselves show evidence of fraudulent activity, such as visible attempts of tampering of third party documents being examined by the FI, or the inclusion of falsified documents. Such reviewing and escalations require highly experienced staff members to make such calls, and it is recognised that such resources are becoming less and less available in the workforce.

6.2 Partially automated identification of collusion risk

Some partially-automated approaches are currently used in the industry. These technology solutions screen transaction details through a set of automated conditions to establish whether or not a transaction is in line with the client's line of business as noted during the KYC process, and whether or not the transaction itself appears to have any fraudulent characteristics. These solutions will still rely on human intervention to investigate exceptions before a judgement call can be made on the materiality of fraud risk.

6.3 Automated identification of collusion risk

Collusion is seen as a driving factor in cross-border trade fraud and typically manifests itself through common ownership between the buying and selling entities.

From a CDD perspective, the client relationship is owned by the FI's client relationship or coverage business line and the products/services offered to the clients will be managed by separate functions within the FI.

A robust initial CDD/KYC process is essential in understanding the client, business sector, expected activity, the goods it trades, the countries it deals with etc. Even if the counterparty were to be banked by the same FI in another country, the CDD information held for each client cannot be shared across borders due to data sharing restrictions.

[2] Financial Crime Guide published by the Financial Conduct Authority (Release 35 - April 2024)

Hence, trade finance staff within an FI's local branch may not be as familiar with the key officials, partners, directors, sole authorised signatory, authorised representative, ultimate beneficial owner, key controllers, etc., any one or more of whom might be the common link in any shared ownership between the client and counterparty.

Furthermore, while CDD information for the client would be available internally to the FI, there would be little or no data available on their client's counterparty (unless the counterparty is another client of the same FI in the same country, typically only available to the largest of FIs).

Most of the more sophisticated and systemically important FIs will have invested in post-transaction automated monitoring solutions using Social Network Analytics and Big Data techniques including Large Language Models (LLM) and Gen AI to identify common ownership structures, whether known or undisclosed to the FIs which may pose a risk. Technology solutions such as Espero, Quantexa, BAE Systems and IBM have partnered with major FIs in this space.

6.4 End-to-end control fraud detection ecosystem

The Taskforce envisions FIs generally moving away from manual processes as adoption rates for new technology solutions continue to improve, grow and evolve in the fraud detection ecosystem. In the short term, any manual approach should therefore be coupled with a robust initial CDD/KYC process and appropriate linkages to post-transaction financial crime detection models which evaluate corporate ownership structures and payment flows to assess the risk of collusion mapped to payment anomalies. The significant cost associated with the implementation and use of these technologies makes it a challenge for smaller FIs to adopt these solutions. An appropriate fraud prevention ecosystem may range from minimum deterrence through risk awareness coupled with enhanced due diligence to technically advanced systems capable of contextual monitoring at a holistic client level.

7 Solutions and best practices

7.1 Enhanced due diligence (EDD)

EDD for higher risk clients should include among other requirements, the plotting of common ownership patterns to identify with the potential risk of collusion which in turn could determine how the FI classifies the risk associated with clients and thereby the frequency and strength of any applicable controls.

Valuable data insights around anonymous or opaque corporate structures must be made available to FIs, regardless of systemic importance or sophistication, so they are able to positively match beneficial owners and key controllers within a wider pool of entity level information that is publicly available (for instance through an API connection from CH or NECC's JMLSG partnership). This would enable the creation of a viable and sustainable fraud risk control framework which not only addresses the need to exclude bad actors from entering the financial system, but also provides FIs with the necessary tools to proactively engage to prevent fraud rather than only seeking to reactively redress the consequences of fraudulent activity impacting the financial system.

7.2 Adoption of an end-to-end control framework

Effective EDD/CDD measures can detect the potential risk of collusion. If trade is digitalised, FIs will be better placed to leverage new technology solutions to manage how product and transactional risk can be mitigated or tailored to map against vulnerabilities.

- **Pre-facility:** This would typically relate to a tailored risk-based approach towards understanding the client and creating improved client profiles by mapping out their typical transactions and financing requirements. It would also be prudent to identify how these fit in with the business models of the various related entities as also with respect to the broader client group, particularly when these related entities are banked by a single FI.

- **Transactional:** Manual transaction reviews would typically focus on the detection of potential documentary fraud. From a digital trade processing perspective, product level controls would be mirrored in rules developed to flag and prevent the straight through processing of potentially fraudulent transactions together with money laundering and sanctions risk indicators.

- **Post-transaction monitoring:** The use of standard rules-based algorithms in transaction screening/ monitoring platforms and/or contextual monitoring models using new technologies and threat detection capabilities can help prevent fraud. Any collusion risk identified at this stage can be mapped against actual payment information which would have been missing at the pre-facility stage. This leads to a much clear visualisation of expected activity against actual activity.

- **Unusual or suspicious activity reporting:** Any unusual and/or material risk identified at each of the above stages should result in an escalation through an appropriate channel to relevant fraud risk management teams/individuals within the FI having the necessary delegation of authority / competency/subject matter expertise. SAR filing to the authorities (FIU) should be completed on behalf of the CMLCO/MLRO in a timely manner once assessed and approved by them.

- **Procedural guidance:** Adequate and clear guidance should be available on the timely detection of high-risk indicators at every stage of the transaction/client lifecycle. This would demonstrate reasonable attempts made by FIs engaging in trade finance to raise and maintain awareness around documentary risk. From a dedicated risk management perspective, threat detection models should seek to assess fraud risk across relevant elements of the client profile (CDD/ EDD profile); the client financial/credit profile; counterparty profile; and transaction profile.

- **Lessons learnt:** The identification of fraud risk through escalation should result in key findings which must be shared across the FI's risk and control framework as part of an ongoing lessons learned initiative. This in turn could define control enhancement/optimisation at one or more stages during the transaction/client lifecycle plus help with the detection of emerging fraud risk, if any. Circulation of key findings and lessons learned from NECC's JMLIT partnership to FIs on a regular basis are appreciated and provide the industry with opportunities for ongoing enhancement of fraud controls in response to the evolving nature of criminal intent, methodology and activity.

8 Conclusions

This summary focuses on the challenges associated with the implementation of fraud controls for FIs engaging in trade finance. The summary concludes that, while a relatively robust fraud risk ecosystem can be developed for use within most FIs, this is not achievable without there being a shift in regulation addressing the permissible transparency in corporate ownership structures. As such, the industry practice of relying on FI self-assessments to gauge risk appetite for loss remains the standard, based on which fraud prevention controls of varying types are employed.

There is without doubt a clear desire for technology to lead in this space. The recent industry paper from ITFA1 outlines the various approaches, solutions and technology vendors available to FIs for addressing trade fraud risk. However, the challenges outlined in this paper continue to exist and it is only pursuant to more heightened focus from industry practitioner groups (i.e. BAFT, ICC, Wolfsberg) and the sharing of fraud risk information by NECC's JMLIT partnership, that any wider industry level attempt would bear material outcomes in the prevention of fraud.

[1] ITFA'S Fraud Prevention Working Group releases first white paper, May 2024

Acknowledgements

4

Trade Digitalisation Taskforce

The Trade Digitalisation Taskforce was launched in 2023 as a public, private partnership forum that acts as an impartial, solution focused, systems thinking forum that brings together the International Chamber of Commerce ambition to digitalise world trade and reduce the trade finance gap with the government ambition to increase UK growth and productivity.

Its remit is to promote and implement the benefits of trade digitalisation, remove financial regulatory barriers, prevent fraud in trade, reduce KYC bureaucracy and establish digital identities for cross border trade. The taskforce is co-Chaired by the Minister for Exports at the Department for Business and Trade [DBT], ICC United Kingdom and Barclays. The taskforce meets quarterly and presents practical recommendations to government that are scalable internationally.

The taskforce brings together financial institutions, industry, regulators and wider stakeholders and includes the International Centre for Digital Trade and Innovation, largest international trade banks and business organisations based in the UK, international institutions such as the ICC Digital Standards Initiative, Global Legal Entity Identifier Foundation, International Trade and Forfeiting Association and Baft as well as His Majesty's Treasury and DBT.

Acknowledgements

This paper has been written for the Trade Digitalisation Taskforce.

With special thanks to the HSBC, Standard Chartered Bank and Barclays financial crime compliance and trade finance teams for initiating the paper.

ICC United Kingdom is the representative voice for ICC in the UK and provides a mechanism for UK industry to engage effectively in shaping international policy, standards and rules.

We are the leading voice on digital trade ecosystems, act as the ICC representative to the Commonwealth and Co-Chair the Legal Reform Advisory Board at the ICC Digital Standards Initiative.

iccwbo.uk @iccwboUK /ICC United Kingdom info@iccwbo.uk

#WeAreICC

ICC United Kingdom
Registered office: First Floor, 1–3 Staple Inn, London WC1V 7QH
Company number: 10763507 VAT number: 42209200