Asia-Pacific Economic Cooperation

APEC Business Advisory Council

Asia-Pacific Financial Forum Digital Trade Finance Lab

Combating Trade-Based Money Laundering Whitepaper

Recommendations and Key Asks to APEC Finance Ministers

Publication Date: June 2021

Working Group Convenors: Henry Roxas and Mathias Berthelemot from R3

Combating Trade-Based Money Laundering (TBML)

Foreword

The Asia Pacific Financial Forum (APFF) is uniquely positioned to bring together both the private and public sector, educate the broader industry, and provide a platform for the industry to identify more efficient and effective means of combating TBML.

The genesis and context of this Whitepaper is an initiative under the APFF Digital Trade Finance Lab ("APFF Lab"), which created a TBML Working Group to undertake the specific ask from APEC Finance Ministers, as stated in the annex to their 2020 Joint Ministerial Statement that "APEC member economies look forward to an update on the project regarding the use of technology to combat Trade-Based Money Laundering."

The APFF Lab intends to convene discussions to review the Whitepaper with relevant stakeholders and will welcome the participation of APEC Finance Ministry and Central Bank Officials in these discussions.

Special acknowledgements go to R3 - the Working Group convenor – as well as the institutions and their representatives that participated in the Working Group that contributed to the Whitepaper including:

- Henry Roxas and Mathias Berthelemot from R3
- Steven Nichols and Stacey Facter from BAFT
- Kevin Carr from Finiden
- Tat Yeen Yap from MonetaGo (Co-Sherpa, APFF Digital Trade Finance Lab)
- Maarten Stassen and Clark Jennings from Crowell & Moring
- Radish Singh from Deloitte
- Mark Borton from National Australia Bank
- Matthew Field from NICE Actimize
- Marc Smith from Conpend
- Colin Camp from Pelican
- Vyas Abhishek from ANZ Bank
- Sriram Muthukrishnan from DBS Bank
- Minli Ng and Samuel Mathew from Standard Chartered Bank
- Alexander Malaket from Opus Advisory
- Edward Young from HSBC
- Akika Ichiki from Mizuho Bank
- Julius Caesar Parreñas from Daiwa Institute of Research (APFF Coordinator)
- David Bischof from the ICC Banking Commission (Co-Sherpa, APFF Digital Trade Finance Lab)
- Steven Beck and Catherine Estrada from the Asian Development Bank
- Alexey Kravchenko from the United Nations ESCAP
- Joel Gibbons from Canada Border Services Agency
- Matthew Shannon from Finance Canada's Financial Sector Policy Branch
- Charlotte Kan, Independent Editor

Brief

- Our working group is composed of private sector banks, trade experts and technology providers located and working in APEC member economies. Our discussions focused on what would be the most effective ways to combat TBML.

- Our paper concludes, reflecting the broad consensus within the working group, that emerging technologies such as Blockchain, Artificial Intelligence and Secure Multi-Party Computation can alleviate many of the compliance issues with regard to private-private information sharing needed to facilitate an industry-wide and cross-industry response.

- We also highlight some existing use cases for Blockchain and AI for the automation of TBML monitoring and currently available privacy-enhancing technologies that can alter the typical trade-off between the security and availability of information, and thus between privacy and preventing illicit finance. These technologies can provide the automation and information sharing that industry participants are seeking while also accommodating the understandable privacy concerns of APEC member governments.

- Our group asks that Finance Ministers and regulators provide the necessary intergovernmental coordination, regulatory clarity, and space to adequately test, develop, and implement these ideas using these Blockchain, AI and privacy-enhancing technologies such as Secure Multi-Party Computation.

Executive Summary

Trade-Based Money Laundering (TBML) is defined by the Financial Action Task Force (FATF) as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins".[1] The complex web of transactions involved in global trade makes it easy for money launderers to obscure the origin of their funds. TBML is a significant issue that is affecting every region of the planet. As a key player in global trade, APEC is vulnerable to criminals that exploit the intricacies and sheer volumes of trade flows to launder their illicit proceeds through the region's financial systems.

Unfortunately, regulators and financial institutions (FIs) face many challenges in combating TBML. One of the unique challenges faced is the lack of and necessity for coordinated efforts between private and public players to effectively capture instances of TBML.

In addition to the need for public-private sector collaboration, developments in private-private information sharing, data analytics, and emerging technology can go a long way towards enabling greater private-public collaboration in the fight against TBML. Technology such as Secure Multi-Party Computation, which protects data privacy can enable cross-border, private-private trade data information sharing while remaining compliant with applicable regulations. The APFF can play a role in improving the effectiveness of implementing TBML controls.

The working group considered the various open literature, industry guidance on TBML including but not limited to the Financial Action Task Force (FATF) and FATF-style Regional Body (FSRB) documents focusing on TBML, such as the 2006 landmark study, the 2008 best practices paper, and the 2012 report by the Asia Pacific Group on Money Laundering (APG), including the BAFT and ICC publications.

This Whitepaper discusses general TBML challenges and focuses on one specific source of TBML risk – fraudulent invoices - and explores how information sharing as a key success factor in combating TBML is constrained by legal challenges and policy considerations. It then discusses the specific role of data and emerging technology in addressing the challenges. Finally, it makes a series of recommendations – "Key Asks" – for APEC Finance Ministers to consider adopting.

> It is our view that TBML is a significant problem that only collaboration and innovative approaches can solve.

[1] FATF Trade-Based Money Laundering Trends and Developments http://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

I. TBML Challenges

Overview of General TBML Challenges

Financial crime is a huge and widespread problem. The amount of money laundered globally in a single year represents about 2 - 5% of global GDP, or circa 2 trillion USD, estimates the United Nations Office on Drugs and Crime (UNODC).[2] To combat it, banks and other financial institutions spend billions of dollars on compliance every year - or risk paying billions in heavy fines and penalties.[3] However, the results of these efforts on TBML are limited, with only a fraction of global illicit financial flows interdicted (< 1%).[4] APEC is a key player in global trade. This makes the region vulnerable to criminals that use the complexities and sheer volumes of trade flows to launder their illicit funds through the region's financial systems. Over/under invoicing, or invoice tampering, is a major TBML scheme. ESCAP estimates that the Asia-Pacific region loses at least 3.8 per cent of tax revenues to such invoice fraud.[5]

Trade Finance, a Key Source of Money Laundering

With contribution of 38% of the world's population, 60% of the world's GDP and 47% of the planet's trade of goods and services, the APEC region is an engine of global trade.[6] Unfortunately, the financing mechanisms that support global trade are attractive to money launderers and financial crime. For this reason, trade finance is viewed by regulators and standard setting agencies as risky for money laundering and other financial crimes such as terrorist financing and breach of sanctions.[7] "Financial institutions have been facing much difficulty in monitoring and implementing controls in their trade finance business to combat trade-based money laundering. The problem has been further exacerbated by lack of clarity in the compliance requirements and regulatory expectations in many jurisdictions," Deloitte said in a recent report on Trade-Based Money Laundering Compliance.[5]

The Documentary and Open Account Trade Gaps

Currently, around 10% of trade is documentary where banks intermediate the flow of transactional documents between buyers and sellers.[8] Much of the rest is on 'open account' basis, where buyers and sellers do not rely on banks for document flows, and a bank's role is often limited to the processing of payments. Banks therefore have limited visibility of the underlying trade transaction to identify suspicious activity. There are also prohibitions against, or no common standards established today, to mandate or manage exchanging trade data between banks and with other organizations. What the limited visibility and barriers to

[2] United Nations Office on Drugs and Crime (UNODC), Money Laundering, https://www.unodc.org/unodc/en/money-laundering/overview.html
[3] KPMG, Combating financial crime, 3 focus areas for banks to achieve more effective and efficient customer due diligence https://home.kpmg/xx/en/home/insights/2019/03/combating-financial-crime-fs.html
[4] BAFT, Combating Trade Based Money Laundering – Rethinking the Approach https://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paper.pdf
[5] United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). Financing for Development in Asia and the Pacific: Highlights in the Context of the Addis Ababa Action Agenda – 2019 Edition (p 10). Available at https://www.unescap.org/resources/financing-development-asia-and-pacific-highlights-context-addis-ababa-action-agenda-2019
[6] Asian-Pacific Economic Cooperation, APEC in Charts 2019 https://www.apec.org/Publications/2019/12/APEC-in-Charts-2019
[7] Deloitte, Balancing the Act of Trade Based Money Laundering Compliance, by Radish Singh https://www2.deloitte.com/kh/en/pages/financial-services/articles/tbml-compliance.html
[8] International Chamber of Commerce ("ICC") https://safety4sea.com/wp-content/uploads/2020/07/ICC-Global-survey-on-trade-finance-2020_07.pdf

the exchange of data presents is a structural issue in the combat against TBML. To overcome such structural challenges, one key is for regulators to set some compliance expectations on data sharing and TBML controls.

Combating TBML: A Responsibility of the Whole Ecosystem

Today, it might appear that regulators expect banks to play a significant and almost sole role in the identification of suspicious activity. However, given that in open account trade finance transactions, banks have limited visibility and/or access to documents accompanying the transactions, banks will need to rely on more than just transactional information if they are to identify suspicious activity. For the identification system to become increasingly more efficient, additional stakeholders are needed to share the burden; they are such as:

- Shippers and shipping companies
- Shipment Inspectors
- Brokers
- Logistics providers
- Government e.g., Customs
- Auditors
- Insurers

Screening for Invoice Fraud to combat TBML

The Wolfsberg Group, an alliance of global banks working together for the development of frameworks and guidance for the management of financial crime risks, refers to methods for moving illegal funds.[9] One such method commonly used is misrepresenting the price, quality, or quantity of goods by over- or under-invoicing, multiple invoicing, short- or over- shipping, obfuscation (shipping something other than what is invoiced) or phantom shipments (shipping nothing at all).

Red flags are already defined by various parties and were aggregated by BAFT (Bankers Association for Finance and Trade) in its *Guidance for Identifying Potentially Suspicious Activity* for ease of understanding.[10] The approach to assessing these red flags requires greater clarity in terms of standards and acceptable practices. Given the lack of clear standards, FIs have instituted different practices to tackle the risk; these have proven very costly when measured against the level of effectiveness.

To address these red flags, it is possible for price and classification of goods to be vetted via the use of secure data sharing and screening technologies so that the pricing may be more accurately vetted, or at least tested for reasonableness. This will significantly improve efficacy of risk management. Including third-party data classification systems such as the Harmonized System (HS) or equivalent to better identify goods pricing could help train the Artificial Intelligence (AI) models under development by many financial institutions.

Technologies such as text-based mining, can be used to help predict, classify, and standardize invoice data, facilitating processing of data from different sources.

[9] ICC, Financial Crime Compliance Checks on the Price of Goods in Trade Transactions – Are Price Checking Controls Plausible? https://iccwbo.org/publication/financial-crime-compliance-checks-price-of-goods-trade-transactions-price-checking-controls-plausible/
[10] BAFT, Guidance for Identifying Potentially Suspicious Activity http://www.baft.org/Handlers/AptifyAttachmentHandler.ashx?AttachmentID=7r1OKJQloZI%3D

A Need for Joint Standard and Common Policy

Currently, a lack of adequate resources to monitor and interpret trade data properly is a problem further exacerbated by the cross-border sharing of data regulations in certain APEC economies. The ability to share trade-related data, such as goods pricing, may require changes in laws and regulations to address security and confidentiality challenges. Laws around the permissibility of secure cross border sharing of private-private data (among various private sector stakeholder e.g., banks, other financial institutions, shipping companies etc.) is instrumental in the identification of suspected TBML activities.

II. Information Sharing

Sharing as a Key Success Factor in Combating TBML

Today, most trade information sits in silos – they are confined within each organization. This is well known, hindering any industry-wide and cross-industry coordinated effort in detecting TBML. Without a holistic view of information across the end-to-end value chain, isolated controls are built by each participant, which stops them from being fully effective. End-to-end information sharing, particularly of key invoice data such as pricing, originators, and beneficiaries, will help to tackle the problems present on both documentary and open account trade.

Two main challenges in achieving an unrestricted coordinated information flow have been identified:

- The availability of standardized information: Due to the lack of standardization across jurisdictions and amongst the organizations involved, a lot of information is either available in an unstructured form (paper-based) or where available, classified differently within different organizations.
- Privacy and other legal hurdles in sharing information: Due to the sensitive nature of some of the data, there are legal constraints and challenges as well policy considerations to contend with.

The following sections offer potential solutions to address these two challenges and provide some policy considerations to help facilitate the solution:

The need for Standardization of Data

Currently in global trade, while some information standards exist, several gaps remain that would require data exchange across jurisdictions and entities. Some of the key areas where information sharing is essential to prevent TBML include:

a) Invoice / Pricing information (for under / over invoicing)
b) Shipment and financing information (for duplicate financing)
c) Know Your Customer (KYC) information
d) Information on incidents / Suspicious Activity Reports (SARs) / Risk outcomes

This paper focuses on (a) invoice and pricing information sharing.

Price manipulation (under / over invoicing) is a very prevalent typology for money launderers to leverage (noting that collusion is required for this to be effective), and the challenges in accurate benchmarking of pricing information are well acknowledged in the industry. Aside from benchmarking, there are other challenges with the role of invoices in trade transactions:

- The collection and extraction of invoice information
- Non-standard and inconsistently available components of information like goods description, origin information etc. across all trade documents

The following data fields are considered critical for providing trade information to identify potential suspicious activities:

- Buyer / Seller names, addresses, and identifiers e.g., Legal Entity Identifier (LEIs)
- Unit pricing
- Quantity and/or volume
- Grade, specification of goods
- HS codes
- Invoice / Contract numbers
- Currency codes and amount
- Payment terms
- Origin, purchaser, and jurisdiction of goods
- Ship from and ship to ports
- Separated c.i.f. component

Legal Constraints and Challenges of Information Sharing

The other barriers to effective information exchange to be removed include enabling and controlling access to quality information. Bank secrecy and privacy laws in many economies have been put into place to safeguard sensitive information. Information sharing across entities or jurisdictions has been prohibited given the difficulty in establishing controls on who and how information is used.

Newly developing viable technologies could potentially rebalance these interests by offering comparable (or greater) security together with more access to data. Some solutions include the use of blockchain, Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), Secure Enclaves, Zero-Knowledge Proofs (ZKP), and Federated Learning all of which provide differing degrees of security to address data access and controls.[11] Parties providing information can remain in control of the data, have it stored on-premise and access it in real time.

Flagging suspicious activity often involves transactions between banks that are confidential. Solutions like Secure Multi-Party Computation (SMPC) protocols enable these transactions to be shared in an encrypted form, to allow them to remain hidden to the other parties. It offers Remote Attestation (RA), a type of digital key, so parties involved may each audit how the data is being used and ensure that unauthorized entities cannot access it. With a Secure Enclave (solutions built into the CPU, thus providing hardware security) and blockchain, all parties providing information remain in control of the data at all times, as the data remains stored on-premise.

Policy Considerations to Enable Information Sharing

For the standardization of invoice information, governments and regulators could develop minimum standardized information for trade invoices that businesses would have to comply

[11] See Annex A below

with. This would enable information to be shared using otherwise inaccessible data to feed to algorithms that can flag fraudulent behavior.

For this system to work, APEC must have jurisdictions that facilitate smooth public-private and private-private sharing of information. Customs, for instance, hold extremely valuable information that could be pulled into a data bank accessible by financial institutions for price validation, creating an inter-bank information sharing ecosystem.

Potential sharing mechanisms:

- Public / private partnership – Governments could be mandating and supporting information sharing by providing a common platform and rulebook for such information sharing. Customs and enforcement agencies would have a key role to play, due to the amount of valuable information and intelligence they hold.
- Private / private partnership – Similar to the trade finance registry in Singapore, FIs could collectively participate and define the information sharing standards.
- Public / public partnerships – Inter-jurisdiction sharing of information to allow different regions and/or governments to collaborate.
- Any technology used should adhere to existing privacy and security policies for sensible information sharing.

III. Technology

Technology to Combat TBML

Technology has been key over the past years to enhance the fight against TBML. FIs have adopted Optical Character Recognition (OCR) and Natural Language Processing (NLP) technologies to extract data from trade documents, and transaction screening systems - often based on AI algorithms - can flag specific patterns in structured data. However, it is still not possible to create a holistic view of all the various interactions and activities related to a trade finance transaction since each party only has access to a subset of the needed information, significantly hindering attempts to decrease fraud. Emerging technology could fill this need and potentially change this paradigm entirely.

The Importance of 'Good' Data

When it comes to creating effective processes for combating TBML, accuracy and completeness of data is just as important - if not more - than quantity. This is essential to build systems that can identify the critical data required to identify red flags, automate AML rules, and generate alerts to flag other unusual transactions. However, data protection rules and the limitations of cross jurisdiction exchange of information prevent banks and all trade players from accessing what could be vital information. As a result, FIs end up with a lot of unstructured and semi-structured data. Developing an accurate and shared data foundation is essential so it can be shared safely across all the parties in the ecosystem.

The Key Role of Emerging Technology

This is where emerging technology can intervene. It can bridge the gaps between governments' expectations and what is practical today by automating TBML monitoring and providing much greater visibility through secure information sharing. The emerging technologies highlighted below can enhance both the availability, confidentiality, and integrity of trade data.

- A number of banks in Singapore recently unveiled a blockchain proof of concept for a Trade Finance Registry (TFR) to prevent trade fraud. The TFR works as a platform to ease the flow of information between banks and prevent duplicate financing.

- In India, the Reserve Bank of India-supported Trade Receivables e-Discounting System solves for the problem of duplicate invoice financing by deployment of a blockchain platform that keeps a record of cryptographic hashes (instead of actual data) of financed invoices, against which hashes of invoices submitted for new financing requests are checked for matches.

- Many banks around the world are using a combination of OCR and NLP technologies to extract relevant information from unformatted documents and messages, analyze and format it ready for compliance screening and checking. Machine Learning is then used to build models based on historical information and domain data to alert on any anomalies in the trade.

- Several Mexican Banks have also taken up initiatives to exchange KYC and anti-fraud information secured by secure enclaves and zero knowledge proofs.

Unit Price Analysis to Combat TBML

Another example of the importance of 'good' data is unit price verification, which is complex. FIs are often unable to assess the validity of stated unit pricing due to the lack of relevant information (terms of specific business relationship, discounting for bulk purchase, quality of goods, non-publicly traded products etc.)

Thanks to new technologies like blockchain, AI with Privacy Enhancing Techniques (PETs) and OCR (see below), the flagging of anomalies in trade transactions can be automated – and significantly enhanced.[12]

Fig. 1: Utilizing New Technologies to Implement TBML and other Financial Crime Programs

	Pre-Transaction		Transaction Processing			Post-transaction	
New Technologies	**Product selection**	**Data entry**	**Workflow management**	**Document checks**	**Compliance checks**	**Problem resolution**	**Client management**
Optical Character Recognition (OCR)		**Text recognition** from trade docs to minimize data entry					
Artificial Intelligence (AI)	**Enhanced KYC** (e.g. web scrape)	**Use of NLP** to analyse, perform contextual analysis, format & **normalise unformatted data**		**Cross reference trade docs** to improve accuracy of data field extraction	**Use of ML to build models** based on standard behaviour & patterns to **identify potential red flags**		
Internet of Things (IoT)			IoT data source to **track physical movement of goods as input to fine-tune AML transaction monitoring systems** (e.g. suspicious shipment routes, goods sourced from/to sanctioned country)				
Distributed Ledger Technology (DLT)		Replace doc check, data entry, validation w/ **single digital record**	**Exchange of trade documents** between counterparties, **validate authenticity,** completeness & conformity of trade docs to T&Cs. **Auto release of payment** based on trade data.		Create **smart contracts** to **raise red flags** based. Mutualize the cost of checking for dual use goods within a network.	**Smart contract** to auto-create and submit **Suspicious Transaction Reports (STRs)**	
Secure Enclave			Use of secure hardware and software for enhanced data protection controls. **Pool private trade documents** to perform calculations on **unit price analysis** while **keeping data private.** Aggregating trade data **to fine-tune transaction monitoring systems, reduce false-positive red flags and manual checks**				
Secure Multiparty Computation (SMPC)				Allows two or more parties to analyze combined data without sharing underlying data with one another. Does not require secure hardware as in Secure Enclave. For example, **can analyze trade transaction datapoints across multiple institutions to evaluate abnormalities in price and quantity**, without seeing the underlying, encrypted data.			

Adapted from Bain & Company, R3 Analysis

[12] See Annex A below

IV. Key Asks

Our Recommended Solution

To step up the fight against TBML, we recommend a focused effort to facilitate the sharing of information among FIs using new technologies to maintain the appropriate balance between data availability and security. In facilitating information sharing, we believe efforts should emphasize helping industry navigate the issues of data standardization and privacy regulations both within and across economies. Technologies should maintain or improve data security while increasing data visibility so that businesses, and FIs in particular, can comply with relevant regulations, while minimizing costs and administrative and compliance burdens. We also advocate the use of existing instruments in trade players' toolboxes to help them comply with existing regulation.

Our proposed solution outlined in Figure 2 below aims to assist with risk rating or red flagging potentially suspicious transactions, by setting up a trade pricing information sharing utility.

In order to do this, critical and standardized data for trade transactions is needed, such as:

- Price
- Volume
- Origin/destination
- Seasonality
- HS code
- Quality/grade
- Model
- Brand
- And more…

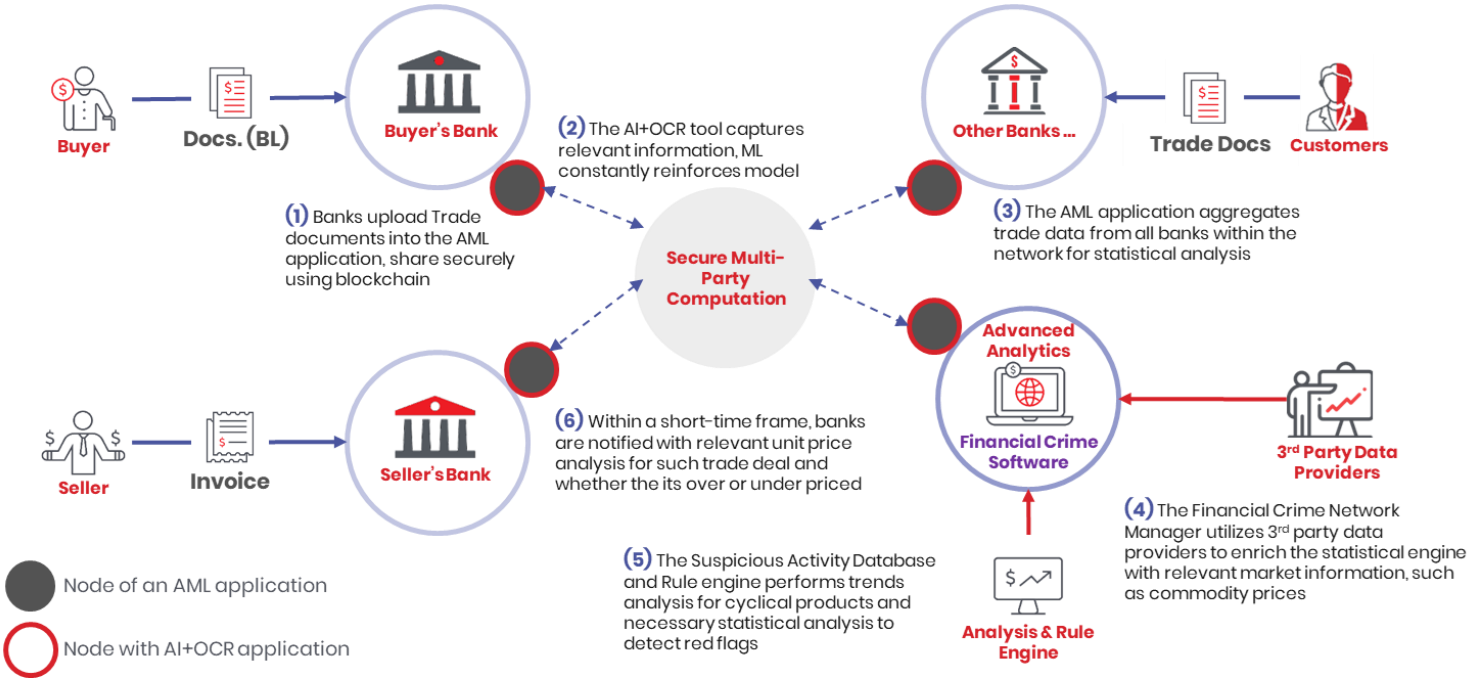
Solution overview

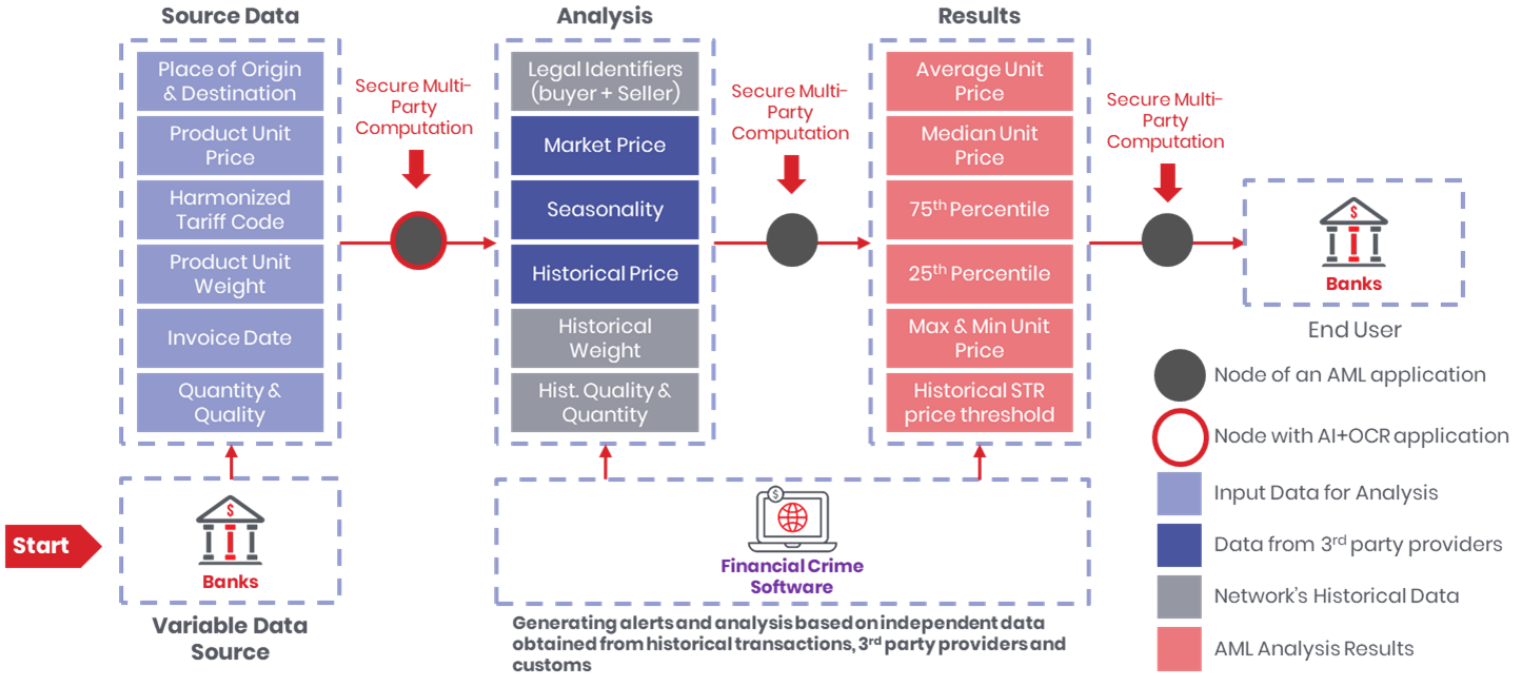
- Sharing trade data through blockchain and other technologies to facilitate greater transparency, secure data, and create more effective monitoring. Data could be processed inside a secure enclave and encrypted for confidentiality and security purposes.
- AI-powered transaction checks and invoice fraud risk flagging of the shared registry.

Participants

- FIs
- Government e.g., Customs (where data is not publicly available)
- Logistics providers
- Shippers and shipping companies
- Certificate providers
- Traders
- Inspectors of goods
- Technology providers
- Insurers

Fig. 2: Proposed Solution: Unit Price Analysis - *Illustrative*





Our Asks to the APEC Finance Ministers

To enhance information sharing, our recommendations are the following:

- Encourage the creation of a regulatory sandbox for TBML:
  - By ensuring regulators understand how the technology works and how it addresses privacy and security concerns, how it complies with existing laws, and get their approval/onboarding.

- Explore government-to-government (G2G) mechanisms to collaborate, such as MOUs or joint initiatives, to enable financial services data connectivity.
  - E.g., the joint statement announced between U.S. Dept of Treasury and Singapore Monetary Authority;[13] The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific to enable seamless exchange of data between customs and tax offices across economies while also reducing trade transaction costs.[14]

- Encourage international standards to first be deployed locally.
  - E.g., HTS codes, standardized invoice data.

- Encourage economies/jurisdictions in which customs data is not publicly available to disclose this information, and if not, to participate in the solution as a data sharing member.
  - A survey could be deployed about data availability.

- For those economies/jurisdictions in which cross-border data sharing poses a legal problem:
  - Phase 1: Align terminology with regulators.
  - Phase 2: Raise awareness about technology as a tool to comply with existing regulation.
  - Phase 3: "Crash test" the technology in the sandbox, use external audits to check security and privacy compliance.
  - Phase 4: Based on findings on the test, change policy and legislation recommendations if required.

- Seek a continuous improvement and feedback cycle:
  - Encourage regulators to regularly share (say quarterly) most recent trends or emerging typologies observed in TBML in their jurisdiction to enhance awareness for additional diligence including geographies, sectors, goods, etc.

- Work with ADB, World Bank, etc. to direct funding to encourage information sharing and standardization efforts across economies and fund pilot and "sandbox" projects.

[13] US Department of Treasury, United States – Singapore Joint Statement on Financial Services Data Connectivity https://home.treasury.gov/news/press-releases/sm899

[14] The Framework Agreement entered into force on 20 February 2021. As of May 2021, five economies either ratified or acceded to the Framework Agreement, namely Azerbaijan, Bangladesh, China, Islamic Republic of Iran and the Philippines. In addition, Armenia and Cambodia have signed the treaty, and is open to all other ESCAP member States. https://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific

Annexes

Annex A –
A summary table of Privacy Preserving analytical Privacy Enhancing Techniques (PETs)[15]

Technique: (Partial, Somewhat or Full) Homomorphic Encryption (HE)

PET description and benefits	Limitations
Homomorphic encryption is a form of encryption where some operations (like addition, multiplication, or both) can be performed on the ciphertext, and when the result is then decrypted it will have the same result as if the processing had occurred on the plain text. HE allows computations to be run on the encrypted data and then decrypt the result of the computation only.	Traditionally subject to concerns about computational limitations and a lack of widely accepted standards. Early Fully Homomorphic Encryption schemes were exceptionally expensive in terms of computational resource requirements. Recent improvements in these techniques allow for some computations to be completed in relatively short order (seconds and minutes), enabling the practical application of homomorphic encryption to protect sensitive data. Likewise, there are initiatives underway (e.g., Homomorphic Encryption Standardization) to define community standards for HE.[16]

Technique: Secure Multi Party Computation (SMPC)

PET description and benefits	Limitations
SMPC, or multiparty computation (MPC), is a subfield of cryptography concerned with enabling private distributed computations. In particular, it may be used when two or more parties want to carry out analyses on their combined data but, for legal or other reasons, they cannot share data with one another. MPC can also be used to allow private multi-party machine learning: in this case, different parties send encrypted data to each other and they can train a machine learning model on their combined data, without seeing each other's unencrypted data.	Current SMPC systems have relatively high communications costs. SMPC protocols often require a high degree of specificity to the use case, making them hard to generalize. They can also be slower than computing on raw data and are contingent on the availability of the parties involved. However, 'compilers' that abstract the underlying protocols to enable general-purpose computing are reported as under development, supporting data science and machine-learning applications more broadly.

[15] Reprinted from Future of Financial Intelligence Sharing (FFIS), Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime. https://www.future-fis.com/the-pet-project.html

[16] See also Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR) iarpa program - https://www.iarpa.gov/index.php/research-programs/hector

Technique: Trusted Execution Environments (TEEs)

PET description and benefits	Limitations
TEEs, or secure enclaves, are a secure area within a physical processor where the processing that happens in that area is hidden from the rest of the processor. TEEs could be used to allow a proprietary algorithm to be run by an untrusted party while ensuring the untrusted party cannot see the algorithm. TEEs often perform and scale well with data size. The technology is commercially developed with Intel's Software Guard Extensions (SGX)™ providing a leading example of enclave computing in Skylake™ processors and their successors. Virtualization of SGX is an emerging capability. ARM's Trustzone and AMD's Platform Security Processor also offer TEE capability. Multiple cloud providers offer SGX hardware where one can run these applications when one does not have direct access to such hardware. Microsoft supports Azure Confidential Computing program; IBM Cloud provides machines with SGX support and Alibaba Cloud has SGX machines as well.	Use of enclave computation may require the use of specific hardware that includes enclave features. For example, Intel(R) SGX™. Some TEE providers enable virtualization as well, but only virtualization on top of TEE-equipped hardware. TEE is considered to be at a relatively high state of technology readiness as a PET. However, much of what an end user expects in terms of usability of a computing product is still very early in development for TEE. A key shortfall at this point in time is the lack of easy-to-use development environments for TEE, which would enable general programmers to use these capabilities efficiently and configure them correctly. Another current shortfall is that leading TEE's such as Intel SGX require interaction directly with the technology provider in order to properly use these security capabilities. TEEs may be vulnerable to certain kinds of side channel attacks. This is where an attacker monitors certain properties of the system, such as the time required to perform an operation, to learn sensitive information.

Technique: Zero Knowledge Proofs (ZKP)

PET description and benefits	Limitations
ZKPs are a method by which an entity can prove that they know something to another entity, without revealing anything other than that they know that thing. ZKPs can be used for authentication. An entity can prove they know a password that proves their identity, without having to reveal their password. ZKP has applications across a variety of use cases – including payments (Zcash), internet infrastructure (NuCypher), digital identity (Nuggets) and others. and it is expected to be a critical enabler of distributed ledger technologies more broadly.	ZKP has only recently seen real-world operational uses as the methodology continues to mature. Scalability can be a technical challenge and, as is common for PETs in 2020, further work is required to develop global community standards for the technology.

Technique: Federated Learning

PET description and benefits	Limitations
In traditional machine learning data is centralized and brought to the model. In federated learning the data is distributed, and the model is sent to the data. What is then centralized is the model updates from all of the federated devices. Federated learning allows a model to be updated without centralizing the data the update is based on. As the central party does not see the data, they need to be confident that the data is structured, cleaned, and encoded appropriately, otherwise it can fail or lead to a poorly trained model. Federated learning is developed and in use in household mobile applications. In March 2019, TensorFlow (a widely used open-source library for machine learning) published TensorFlow Federated, an open-source framework that allows machine learning to be performed on federated datasets.	Federated learning in isolation is not necessarily privacy preserving, as it can be applied in a manner that there are no meaningful privacy guarantees of the models or of the underlying data. It is also important to note that this model does not necessarily produce an equivalent model to the one that would be derived by first combining the training data into a central location; in most cases, a model trained through federated machine learning would be inferior to the one trained on a centralized dataset. Again, one of the challenges being faced is the absence of standards, systems, and homogeneous languages, which permit distinct actors to interact with services based on this technology.

Annex B –
Acronyms used in this paper

Acronym	Meaning
AI	Artificial Intelligence
AML	Anti-Money Laundering
APFF	Asia-Pacific Financial Forum
DLT	Distributed Ledger Technology
FI	Financial Institution
HE	Homomorphic Encryption
HTS	Harmonized Tariff Schedule
KYC	Know Your Customer
LEI	Legal Entity Identifier
NLP	Natural Language Processing
OCR	Optical Character Recognition
PET	Privacy Enhancing Techniques
RA	Remote Attestation
SAR	Suspicious Activity Reports
SMPC	Secure Multi-Party Computation
TBML	Trade-Based Money Laundering
TEE	Trusted Execution Environments
ZKP	Zero Knowledge Proofs