How to effectively tackle trade-based money laundering

quantexa

Connecting data | empowering decisions

Quick links:

What we have learnt so far

Combat trade-based money laundering

Example: Complex criminal network

A multilateral approach to AML

Criminals don't wear black hats and a mask like they used to in the movies. They don't creep around with stolen goods in a brown sack over their shoulder. Criminals are well coordinated, creative, and technologically sophisticated, working internationally as part of a complex network.

Finding criminality among the billions of financial transactions placed every day has never been easy. But, what we do know is that their illegal behavior is almost indistinguishable from legitimate business activity.

So, how can we use data to tackle trade-based money laundering?

30% of all money laundering globally is conducted via trade

Regulators, international bodies and compliance professionals have commented that trade-based money laundering is one of the hardest areas to monitor for illicit activity due to its complexity and scale. Scandals in the recent media spotlight, such as the Azerbaijan and Troika laundromats, exemplify how trade is abused by criminals and how financial institutions are failing to spot them.

However, recent advances in technology and analytical techniques are empowering financial institutions to effectively and efficiently detect trade-based money laundering and fight against organized crime.

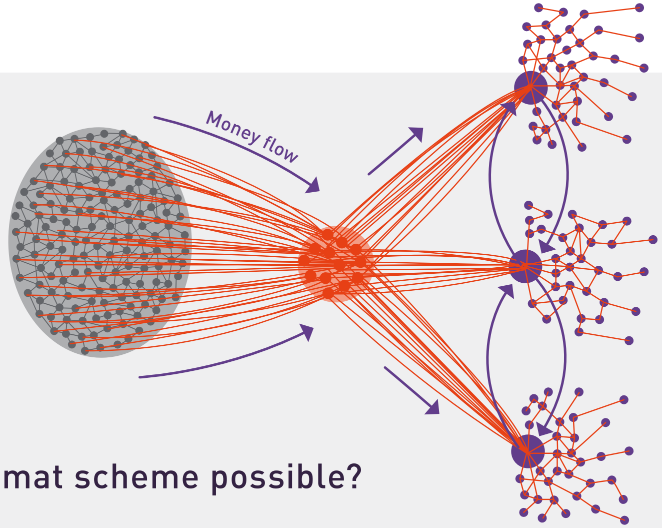
This guide will share insight and observations that Quantexa has collated across numerous projects while identifying suspicious activity and trade-based money laundering using data, including transaction, trade finance documents, third-party sources and more.

The Troika Laundromat was a financial network established by Troika Dialog, a Russian private investment bank, to help its clients move funds out of the country and into the Western banking system. These funds were allegedly used to pay for private jets, custom-built yachts, luxury properties, holidays, private school fees and to make charitable contributions.

According to disclosures made by the Organized Crime and Corruption Reporting Project (OCCRP), it is estimated that **Troika and a network of more than 70 shell companies, enabled the flow of $4.6 billion into the Western banking system and directed the flow of $4.8 billion out.**

Case study

Troika laundromat



How did trade make this laundromat scheme possible?

In addition to mixing legitimately earned private wealth with suspected illicit funds, the scheme used shell companies to complete false trade deals through fake invoices for non-existent goods, which were then purchased by other companies in the scheme.

All the invoices included in the leak documentation published by the OCCRP and its partner news agencies were signed by proxies and sent from a Troika.ru email address. Many of the fake trade transfers took place via Lithuania's Ukio Bank, which was closed by the authorities in 2013.

For example, in May 2004, Ukio transferred $204,000 to a Latvian account to pay for "auto spare parts". The money came from Industrial Trade Corp, incorporated a year earlier in Panama. According to the OCCRP, it had no obvious connection to the car industry, or "food industry equipment", "computers" and "building materials" in which it subsequently "traded" in. Such fake transactions, together with loans and share deals, allowed Industrial Trade Corp to transfer hundreds of millions of dollars.

What we have learnt so far

Trade is complicated. It varies by country, industry and time of year. From the smallest corner shop to the largest multi-national business, retailers to wholesales, manufacturers to supermarkets – everyone engages in trade. As consumers, we purchase the end-products – our groceries, clothes, gadgets – and this is only the tip of the iceberg. All the components that make up a product have also been traded, making up various stages of the supply chain.

There are several steps that banks can take to help manage the risk of trade, including a letter of credit, guarantees, import and export bills, and associated loans and financing. A trade finance contract can cover multiple shipments of products over the course of several months or even years. The goods are delivered by various logistics companies, each with different trade routes, and may continue from distributors to consumers around the world.

The trade market is a complex, global network of relationships between counterparties.

The behavior of money launderers

Criminals who launder their funds through trade range from the naïve to the highly sophisticated. The naïve offenders frequently launder large sums of money, making their activity easy to spot. But this is becoming less common as money launderers become more tech-savvy.

Sophisticated criminals behave differently. They not only run a criminal enterprise, but a legitimate one as well. Contrary to common belief, they file tax returns, pay taxes, complete trade documents with no clerical errors, and operate their business as you would expect a legitimate company to.

This allows criminals to hide their illicit operations in plain sight. If they are using trade to circumvent currency controls, their papers need to be in order so they can move their funds.

How money is laundered

Criminals use a variety of products and companies to launder their funds. Traditional methods include diamonds, jewelry and gold, but any item that can be easily sold can be used.

For example, the latest toy craze means a high demand and an easy way to move the goods. Criminals often buy toys from the legitimate manufacturers and sell them online through eBay or Amazon Marketplace, which don't require a physical shop presence. This can also enable the criminals to generate profit from the mark up on the items sold.

To complete the picture, sophisticated criminals have done their homework on the business and industry in which they operate. The observed transactional activity is well within, or just below, the average transaction value and volume for similar businesses. By acting in the same way as legitimate businesses, money launderers hide from anomaly detection of traditional monitoring approaches.

The transfer of value

At its core, trade-based money laundering is the process of legitimizing funds from criminal activity through the use of trade transaction and the transfer of value. The individual or group of colluding individuals attempts to hide the origins of illicit activities, such as bribery and corruption or human trafficking. This is achieved by transferring value through multiple layers of corporate entities and across various jurisdictions or financial institutions, in apparent legitimate import-exporter trade flows.

Due to the challenges and risk of visibility that are attached to transferring cash, criminals use a variety of means and mechanisms to transfer value through trade. For example, Importer A pays for 10 high-end cars but only five are shipped – this is called a ***partial shipment***. In some cases, no cars are shipped at all.

Over or under invoicing is also used to launder money. **If each car is worth £55,000 but is only invoiced at £5,000, this allows the beneficiary to sell them legitimately at market price without leaving a clear financial trail back to the illicit source of funds.** Often, the trade financing banks are unaware what the large payment is for. These types of transactions generally require collusion by both parties, which is difficult to identify with rules or scenario-based transaction monitoring.

Current systems and controls

Existing transaction monitoring (TM) approaches have failed to accurately detect criminality or produce reasonable and manageable alert volumes. This failure has forced many organizations to adopt a two-pronged monitoring strategy:

1 **For the financed part of trade**
which accounts for 15% of all volume

This relies on human expertise and uses a combination of manual controls and business expertise. Highly trained clerks use simple but effective red flags to spot unusual trades. While some criminals are found, this approach is not systematic and many still slip through the net.

2 **For the non-financed part of trade or open accounts**
which makes up the remaining 85% of all volume

This uses the traditional approach of following simple rules and scenarios to produce thousands of alerts. The majority are false positives, resulting in an increased operations cost and risk, as complex money laundering is potentially being missed.

Complications arise as some of the adopted transaction monitoring strategies have created **monitoring siloes** within the banks. There are separate solutions that monitor the domestic part of trade in their retail AML systems, which often splits SME business accounts from larger corporates and personal customer accounts (such as the accounts of directors with associated business accounts). Any international payments are also monitored in another separate correspondent banking solution, so there is no link between domestic and international transactions. Multiple siloes make it easier for organized criminals to exploit coverage gaps.

Scenarios and behaviors

If we examine the current monitoring typologies and scenarios, the existing transaction monitoring systems have indicators which generate alerts almost continuously – nearly all of these being false positives.

High-risk countries

The majority of trade is involved with high-risk countries. This is because products that we purchase from low-risk countries (e.g. Japan and the U.S.) have parts of the supply chain in high-risk countries.

Most non-western countries appear on a high-risk list so any trade with or between these countries will be flagged as a potential threat. However, there are many legitimate businesses in high-risk countries and banks are there to facilitate this.

Round amounts

This is an uncommon characteristic for domestic retail transactions, but transactions in round amounts are common for international trade, especially for the financed part.

For example, in chip manufacturing, the unit price is low but the volume purchased is high, so typically purchases occur in quantities of 100s, 500s or 1,000s. Loans that are linked to a trade are also usually for a round amount and this varies by industry and country.

Rapid movement of funds

This is another high-risk characteristic in domestic retail but is common for business transactions. Funds are sometimes moved into an account just in time to settle a transaction or have just been paid in by another transaction.

If the company operates internationally, it will have several currency accounts. Money is not left in these accounts for long and is moved to the domestic account used to pay bills and salaries.

Some typologies could be extremely effective but require collaboration

Over- and under-invoicing

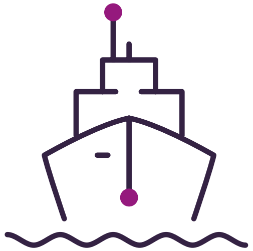
This is the holy grail when monitoring trade – but it requires cooperation and collaboration between governments, law enforcement and banks. The banks do not have enough data to do this accurately alone. It is only in the financed portion of trade (only 15% of volume) that banks see the invoices, bills of lading (BoL), and the price of goods. The remaining 85% happens directly as a payment with no descriptions. Given that each bank only has a portion of the trade in a country, the data points become even rarer.

To effectively assess this, governments need to share information on the average price of goods as the port authorities are the only places that see the bills and invoices for goods entering the country. We have observed that over- and under-invoicing manifests in different indicators, such as U-turns, shared ownership connections between the parties (indicating collusion) and the involvement of shell companies. This means that expensive data harvesting and OCR solutions are not essential in identifying this typology.

Why now?

Criminal are abusing trade from multiple directions

Trade is the lifeblood of the economy; it generates wealth, prosperity and innovation. However, the sheer scale and complexity of trade poses a problem for financial institutions without adequate compliance controls. For example, it is impossible to check every shipping container at the port, making it possible for criminals to use trade to smuggle counterfeit items, endangered wildlife and even people through trade. As banks have created products to help connect importers and exporters, they have unwillingly become conduits for moving criminal assets across borders.



Trade-based money laundering is used as a vehicle for all kinds of crimes

We have observed trade being used to:

- Evade import duties on luxury goods and high-end cars by devaluing them to pay less import tax. However, the price is topped up with additional direct payments, some by circuitous routes.
- Evade currency restrictions and move money out of countries through trade finance products. Typically, goods are over-priced to get the most funds out of the country.
- Enable the movement of corrupt funds. Often people use a variety of companies and goods, from clothing and furniture to precious metals and cars.
- Enable human trafficking – both the physical transportation and the laundering of the illicit funds.
- Violate sanctions, smuggle weapons and help move parts against nuclear proliferation treaties.

How can we effectively combat trade-based money laundering?

Existing systems are failing to scale across the ever-growing amount of data organizations own. With regulators honing in on the trade industry, financial institutions are suffering from larger and more frequent fines for inadequate AML processes. An automated contextual solution is the answer to consistently and effectively detecting financial crime.

- Create context
- Understand trade relationships
- Model complex supply chains
- Identify suspicious activity

1 Create context

By bringing together internal and external data sources, organizations can create a holistic view of trade that includes transactional, customer and counterparty information. Connecting billions of data points through entity resolution provides 360-degree insights on a global scale, enabling a greater understanding of trade relationships and supply chains.

2 Understand trade relationships

Trade is fundamentally a relationship between an importer and an exporter; this relationship is the foundational component for the analysis needed to effectively identify money laundering in trade. It is critical to understand the context of this relationship in respect to:

- Who the importer and exporter is and what they do
- Where they are in the world
- Their size
- Their geographic spread
- Other companies they trade with
- Where they are in the supply chain

3

Model complex supply chains

Supply chains are fascinating and diverse; they don't only involve components of the end product. By using networks to model the complexity of supply chains, you can see there are many trading relationships that may at first seem peculiar but are in fact completely normal.

Here are some examples:

- If we examine mining, a typical supply chain could involve the mining company trading with heavy machinery, machine parts and chemical manufacturers (such as explosives and acids). We are not suspicious of these trade relationships – but why would they do business with a textiles company? The answer could be to buy uniforms.
- Why would a seafood-produce company buy goods from an electronics company? At first glance it doesn't make sense, but it does if the company is buying refrigeration equipment to keep their catch fresh at sea.
- Why would a company be importing rice into Thailand, the world's largest rice exporter? This doesn't make economic sense. However, it does if we know the rice is high-grade Japanese rice used for sushi and sake production, and it comes from Japan from a specialist wholesaler for Thailand.

4

Identify criminal behavior

Criminals are relentless.

We have seen a large number of "phoenix operations" – when one company is shut down or off-boarded then another springs up in its place, often in a different location. In many cases the new company continues to trade with the same counterparties as before, has the same directors and, in some cases, use the same email addresses and phone numbers. Money also flows in the same direction, either into or out of the country, and can be indicative of corruption, bribery, capital flight, or circumvention of currency controls.

Criminals are innovative.

Some criminal organizations buy failing or poorly performing companies with existing international trade relationships and use them to launder funds. What may come as a surprise is they still service their existing customers as the legitimate trade acts as a cover. Criminals also use trade finance fraud to con banks.

It is fundamental for organizations to remain one step ahead of criminals with innovation. Real-time network analytics enables businesses to detect suspicious behavior pre-trade, rather than post-trade. This prevents bad business from entering the bank by stopping fraudulent trades before they occur and mitigating money laundering risk before onboarding.

Trade finance fraud

Criminals not only launder funds through trade but we have also identified that they use trade finance to commit large scale fraud creating huge losses for the bank. Trade finance fraud is a rare occurrence but the losses can be monumental, sometimes upwards of $100 million per incident. By using a Contextual Decision Intelligence platform, you can prevent both money laundering and trade finance fraud.

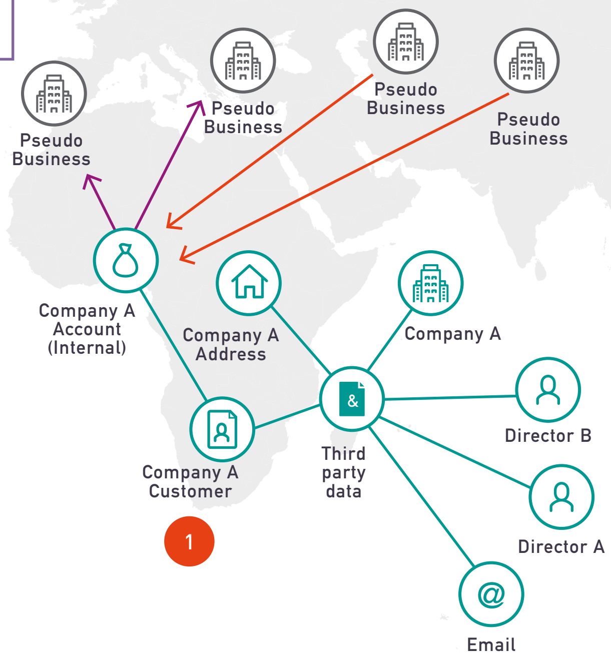
It takes a network to fight a criminal network

Below is an anonymized example of a complex criminal network that enabled the movement of potentially corrupt funds from Africa into Europe.

Key

👤	CUSTOMER RECORD
🏢	BUSINESS ENTITY
💰	ACCOUNT
&	THIRD-PARTY DATA
⌂	HOME ADDRESS
@	EMAIL
👤	DIRECTOR
→	SENDING MONEY
→	RECEIVING MONEY

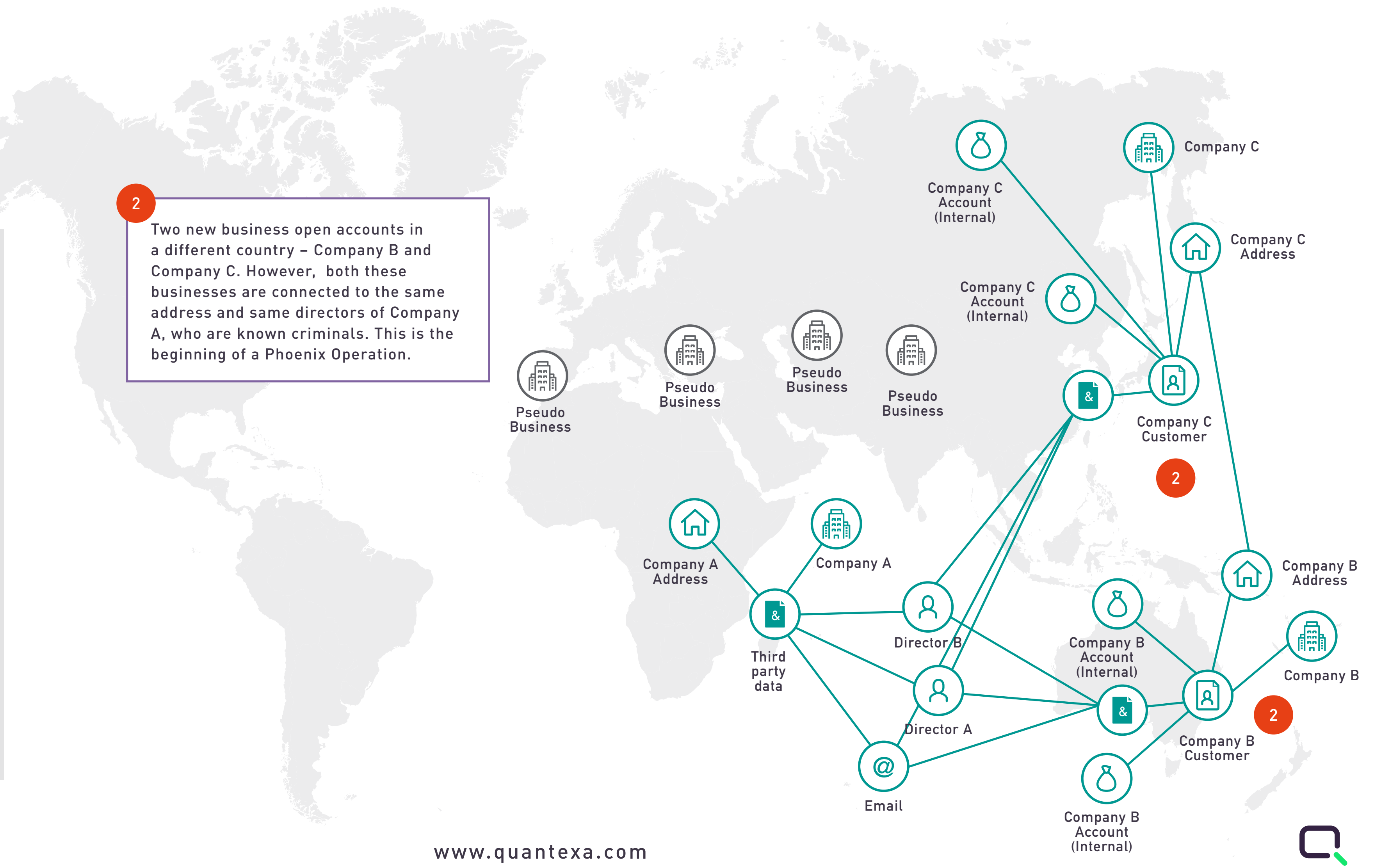
1 Company A is an existing customer of the bank in Africa. This customer had multiple trade relationships, importing and exporting globally. The bank decides to exit the relationship for being high risk.



“ $1.6 trillion of illicit money generated through drug trafficking, human trafficking and illegal wildlife trade is laundered through the global system.”

Key

- CUSTOMER RECORD
- BUSINESS ENTITY
- ACCOUNT
- & THIRD-PARTY DATA
- HOME ADDRESS
- @ EMAIL
- DIRECTOR
- → SENDING MONEY
- → RECEIVING MONEY



2 Two new business open accounts in a different country – Company B and Company C. However, both these businesses are connected to the same address and same directors of Company A, who are known criminals. This is the beginning of a Phoenix Operation.

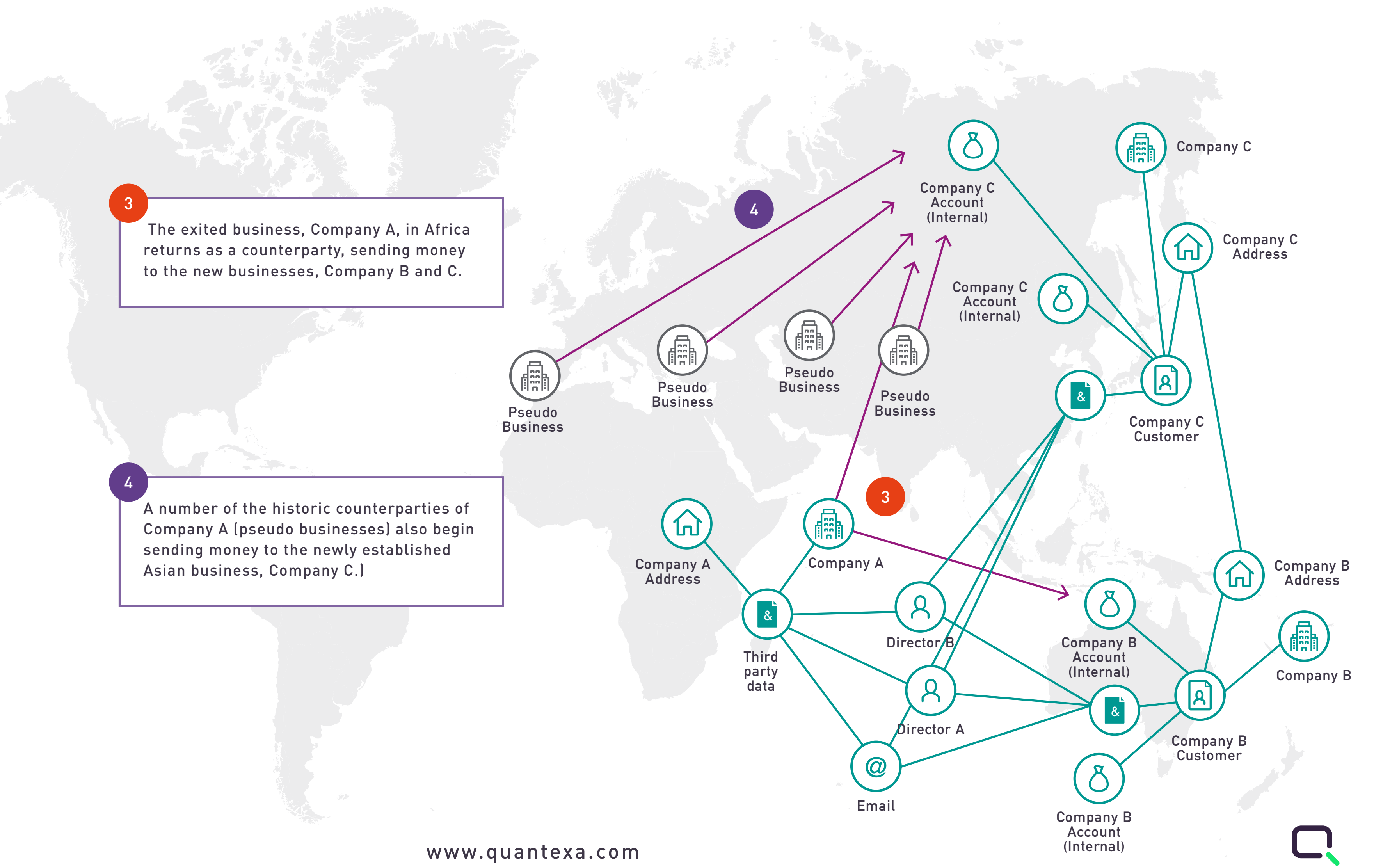
“Less than 1% of these criminals are caught due to inadequate predominantly rules-based AML systems.”

Key

- CUSTOMER RECORD
- BUSINESS ENTITY
- ACCOUNT
- & THIRD-PARTY DATA
- HOME ADDRESS
- @ EMAIL
- DIRECTOR
- → SENDING MONEY
- → RECEIVING MONEY

3 The exited business, Company A, in Africa returns as a counterparty, sending money to the new businesses, Company B and C.

4 A number of the historic counterparties of Company A (pseudo businesses) also begin sending money to the newly established Asian business, Company C.)



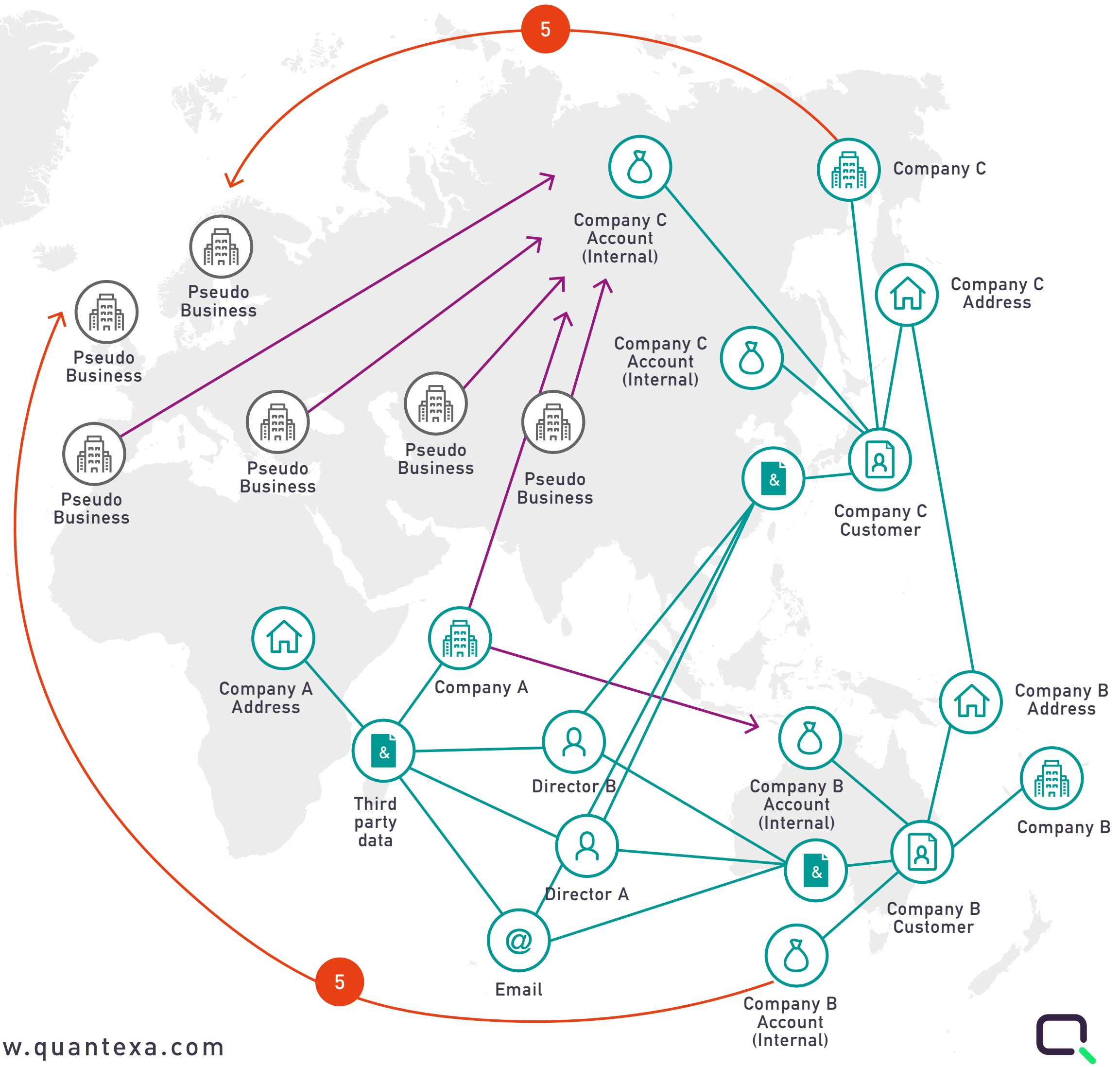
It takes a network to fight a criminal network

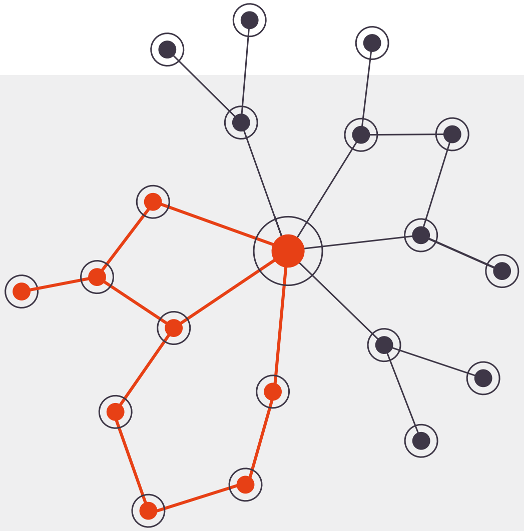
Key

- CUSTOMER RECORD
- BUSINESS ENTITY
- ACCOUNT
- & THIRD-PARTY DATA
- HOME ADDRESS
- @ EMAIL
- DIRECTOR
- → SENDING MONEY
- → RECEIVING MONEY

5 Company B and Company C then send funds to two different countries in Europe.

Internal teams believe that trade finance was used to circumvent export currency control to move funds out of Africa, likely to be corruption.





Case study

HSBC

As the world's largest trade finance bank, HSBC screens over 5.8 million trade transactions a year for signs of money laundering and other financial crime.

> *"This new capability marks a significant milestone in the bank's intelligence-led approach to detecting financial crime. The introduction of the first automated AML capability in the Trade Finance industry enables HSBC to more effectively concentrate our resources on genuine financial crime risk within our business and make trade safer for customers and society."*
>
> Adrian Rigby
> COO of GTRF at HSBC

Challenges

Effectively and efficiently detecting financial crime by establishing where people or companies are acting together to move money around the globe.

Solution

In an industry first, HSBC's Global Trade and Receivables Finance (GTRF) business deployed Quantexa's leading **Anti-Money Laundering (AML)** surveillance system and an automated sanctions checking system as part of its ongoing efforts to improve financial crime detection.

The new AML system uses big data, advanced analytics and automated contextual monitoring to detect and disrupt financial crime in international trade. The contextual approach, developed with Quantexa, builds on HSBC's expertise in network analytics to enable the bank to better identify suspicious patterns and potential criminal networks by combining customer and counterparty trade information, transactional data and external insights.

A multilateral approach is needed to combat trade-based money laundering

To overcome the complex challenges trade-based money laundering poses, companies need to look beyond their own AML programmes. Many professionals within the financial crime and compliance industry, including the **Wolfsburg Group,** agree that greater collaboration and information sharing between public and private sectors is key to mitigate money laundering in trade. This would involve several key international trade players, including shippers, airlines, truckers, port and customer authorities, businesses and law enforcement agencies. Each of these players hold a piece of the trade puzzle.

By working together to build a complete picture of trade flows would help to disrupt criminals. The Wolfsberg Group explain that banks can, and should, remain an important partner for those involved in international trade. Enhancing AML standards and controls will help to detect and prevent trade-based money laundering activity.

Public-private-partnerships

Partnerships, such as the National Crime Agency's **JMLIT** (Joint Money Laundering Intelligence Taskforce) and AUSTRAC's **FinTel Alliance**, have successfully brought together key stakeholders from law enforcement, regulators and financial institutions. These taskforces share information, generate a comprehensive view of how criminals are exploiting the financial system and, most importantly, how these criminal activities can be disrupted.

Entity resolution is the key to successful information sharing partnerships

Given the complexity and inconsistency of trade data, entity resolution is fundamental to bring together all the data from the various organizations within a partnership in order to uncover suspicious patterns.

Dynamic entity resolution is more than linking transactions, trading documents and customer records through a simple process of name and date-of-birth matching. **Within an intelligence-information sharing platform, it would incorporate a numerous internal and commercial data sources and references to an individual or company from several organizations.** This must account for data inconsistencies, errors, abbreviations, and incomplete records and determine whether they relate to the same entity. This is crucial to uncover money laundering and potential collusion by connecting the resolved entities.

Detect hidden risks with contextual monitoring

By implementing controls to effectively tackle trade-based money laundering, financial institutions can make it considerably harder for criminals to move illicit funds cross-border.

You are data-ready now.

You don't need to wait for digitization. You don't need to clean up your data. Quantexa's contextual monitoring solution for trade AML uses dynamic entity resolution to connect your data wherever it is and however it is.

You can reduce manual checks.

Embed human intelligence into your AML systems to improve operational efficiency and reduce manual controls for your staff. Contextual Decision Intelligence helps your organization to process millions of operational decisions more accurately.

You can make trade safer.

Contextual Decision Intelligence enables you to see the relationships between people and organizations. With 95% fewer false positives, you can spend less time and money looking for risk and start finding the bad guys.

Book a demo

Visit our website to learn more about trade AML

www.quantexa.com

quantexa

10 York Rd, London SE1 7ND
200 Broadway, New York, NY 10038

E. info@quantexa.com