

BAE SYSTEMS

INSPIRED WORK

Beware the growing threat of trade-finance based financial crime

George Robbins, senior director, financial crime at [BAE Systems](#), presents an overview of how banks can minimise the risk of fraud and money laundering in their commercial trade divisions. Collusion between buyers and suppliers is a predominant requisite to a criminal's success, and here he discusses how identifying collusion and minimising risk can be practicably achieved



Nikita Starichenko/Shutterstock.com

Counterfeit trade, where criminals make nonsensical or non-existent sales and purchases between entities to transfer money, steal from banks or perpetrate tax fraud, is worth approximately \$600 billion annually. This huge sum accounts for between 5% and 7% of world trade, according to the Counterfeiting Intelligence Bureau of the International Chamber of Commerce Commercial Crime Services.¹ Criminal organisations are circumventing existing regulatory controls with ease, leaving banks vulnerable to trade-based money laundering, fraud, credit risk and tax evasion. What's more, this level of risk is only going to grow, with more banks moving away from saturated investment-grade corporate markets and looking instead for profits by financing small and medium-sized enterprises (SMEs), and by expanding into new geographies.

SMEs tend to offer substantially less public information, financial history and third-party analysis than their large corporate counterparts. This opaque environment provides criminals with a tantalising opportunity to access financing while hiding among legitimate firms. Similarly, varying legal and accounting standards not only increase onboarding costs in new countries but provide more camouflage for criminals posing as genuine businesses.

How can banks minimise this risk?

Data quality is a key problem for banks' compliance operations today. Most banks have built their existing detection systems based on identifying falsified information through comparison of various paper and scanned documents and logical deductions (for example, a shipment route does not match the nature of the transaction). Most banks struggle with the burden of compliance due to poor quality in the vast amounts of detailed information, combined with a shortage of skilled personnel to effectively assess this information. These barriers to automation lead many banks to randomly sample documents, leaving them vulnerable to risks of immeasurable losses and fines.

Regulators have been taking a serious look at this issue. For example, the UK Financial Conduct Authority (FCA) published a thematic review in July 2013 entitled *Banks' control of financial crime risks in trade finance*, warning that "trade processing staff in most banks made inadequate use of customer due-diligence information gathered by relationship managers or trade sales teams."

Criminals, of course, seek to exploit any situation and the more sophisticated criminal groups target the massive volumes offered by international trade and receivables finance by identifying 'red flags' published by regulators, and design malicious strategies to consistently bypass these controls.

Spotting collusion is the key to exposing risk

Whether looking for trade-based money laundering, fraud, credit risk or tax evasion, the key to uncovering these risks is identifying collusion between the participants. Collusion between buyer and supplier is the key to successful financial crime as demonstrated by the scenarios presented in table 1.

While the compliance data requirements are onerous for traditional transaction monitoring, collusion can be identified from a few simple data points. Network analytics to detect collusion require only core deal information: the customer, amount, date, and the counterparty's name, country and bank. This level of data is consistently captured today in operational trade systems for business purposes, and can be easily and consistently leveraged to detect collusion and investigate financial crime.

¹ <https://icc-ccs.org/>

1 Role of collusion in detecting fraud and money-laundering typologies

FATF typologies	Collusion Required?	
	Fraud/credit motive	Money-laundering motive
Over- and under-invoicing	Always	Always
Multiple invoicing	Often	Often
Short and over-shipping	Always	Always
Deliberate obfuscation of goods type	Not applicable	Not applicable
Phantom shipping	Always	Always

However, it is extremely difficult to clarify the actual identity of a bank's deal participants within complex corporate structures and behind deliberate attempts to camouflage identities of company directors and ultimate beneficial owners. This can be achieved, though, by cross-analysing individual and company names against known data such as company registries, credit data and a firm's online presence.

The key is to visualise a company within its corporate group and within the supply chain in which it operates. By aggregating company and individual details with transactional activity, banks can identify a wide range of collusive behaviours: from a buyer and supplier at the same operating address, to complex networks of subsidiaries involved in a wide range of criminal activity. Furthermore, banks can identify round-tripping of funds and complex layering behaviours involving numerous companies and individuals by analysing transactional activity at a network level. A relatively small and well-trained team of specialists can then monitor and investigate collusion across large trade finance portfolios using technology, which networks the data and automatically calculates and prioritises alerts.

The outlook

The business of trade finance and the technology that it uses is increasing in complexity and it is within this complex web of networks that intelligent criminal organisations can best camouflage their collusive misdeeds. As the industry continues to encourage more prolific use of electronic documentation, improved technology from multi-bank platforms, to bank payment obligations, it will continue to fuel banks' expansion into new markets with new clients. Criminals, of course, will use technology to improve their ability to build clandestine networks to disguise illegal transactions, leaving detection of collusion as the most vital tool in the fight against financial crime. Banks will profit only when they can accurately detect financial crime, price the risk and onboard the business that will pay them a reasonable return for that risk.

Contact

George Robbins, Senior Director, Financial Crime
BAE Systems Applied Intelligence
T +44 (0)1483 816000
learn@baesystems.com
www.baesystems.com/ai