THE GUIDE TO ANTI-MONEY LAUNDERING

FIRST EDITION

Editor
Sharon Cohen Levin

CHAPTER 6

Trade-Based Money Laundering and Terrorist Financing

Douglas Greenburg, Eric S Volkman, Benjamin Naftalis and Alli Hugi[1]

Overview of trade-based money laundering

Trade-based money laundering (TBML) describes a set of techniques through which drug traffickers, terrorists and other criminals use the veneer of trade to move illicit funds across borders while disguising the origin and ownership of the funds. One of the most common and sophisticated forms of money laundering, TBML poses significant challenges for law enforcement, financial institutions and other legitimate parties involved in international trade.[2] Although reliably measuring the size of an intentionally secretive business is inherently challenging, estimates of the money involved in TBML run into the billions of dollars annually.[3]

In TBML, criminals manipulate trade transactions to misstate the value of goods or services being traded or conceal the illicit origins of the funds. They rely on techniques such as submitting false invoices, over- and under-invoicing, multiple invoicing, commingling illicit funds with legitimate money and misrepresentation of goods or services. These actions create a discrepancy between the

1 Douglas Greenburg, Eric S Volkman and Benjamin Naftalis are partners and Alli Hugi is an associate at Latham & Watkins LLP.

2 US Government Accountability Office (GAO), 'Trade-Based Money Laundering: U.S. Government Has Worked with Partners to Combat the Threat but Could Strengthen Its Efforts' (4 April 2020) (GAO Report), at 1–2 (https://www.gao.gov/assets/gao-20-333.pdf (accessed 11 July 2023)).

3 See, e.g., 'Trade-Based Money Laundering: A Global Challenge' (A policy memo by Global Financial Integrity, Fedesarrollo, Transparency International Kenya and ACODE) (January 2023) (https://gfintegrity.org/wp-content/uploads/2023/02/TBML-Policy-Brief-Final..pdf (accessed 11 July 2023)).

actual value of the goods traded and the recorded value, allowing funds to move covertly.[4] They also cause illegally derived funds, often bought in currency black markets, to be used in otherwise legitimate commercial transactions.

Criminals leverage TBML to facilitate various illicit activities, including drug trafficking, terrorism financing, sanctions evasion, fraud, corruption and tax evasion. TBML often exploits legitimate supply chains and trade routes, making it challenging to distinguish between legitimate and illicit transactions. The complexity of global trade, involving multiple jurisdictions, different currencies and a wide variety of intermediaries, agents and enterprises – and bad actors – further complicates the detection and prevention of TBML.[5] In 2020, the US Government Accountability Office recognised that 'although TBML is a common form of international money laundering, it is also one of the least understood and most difficult to detect because of its complexity'.[6]

Different countries, of course, rely on diverse regulatory frameworks to target TBML. This chapter focuses on the US system and US enforcement cases to illustrate different forms that TBML takes and how legitimate businesses can become entangled in it – and regulators' enforcement actions targeting it.

The United States' principal criminal money laundering laws, described in the Money Laundering Control Act,[7] have broad application and can result in severe penalties against companies and individuals who knowingly engage in financial transactions involving the proceeds of unlawful activity, including through TBML. These laws can reach companies that engage directly in the criminal activity that generates the illegal proceeds, companies that use otherwise untainted funds for some illicit purpose, or companies unconnected to the original crime that knowingly conduct financial transactions involving tainted proceeds. They also reach those who aid and abet these violations or conspire with others to do the same.

---

4 US House of Representatives, report on 'Stopping Terror Finance: Securing the U.S. Financial Sector' by staff of the Task Force to Investigate Terrorism Financing, Committee on Financial Services, 114th Congress (20 December 2016) (https://financialservices.house.gov/uploadedfiles/terror_financing_report_12-20-2016.pdf (accessed 11 July 2023)).

5 GAO Report (op.cit. note 2), at 5.

6 ibid., at 1.

7 Codified at 18 U.S.C. §§ 1956 and 1957.

To prove a violation of US Code Title 18, Section 1956, the Department of Justice (DOJ) must establish four elements: (1) the defendant conducted a financial transaction; (2) the transaction involved the proceeds of 'specified unlawful activity'; (3) the defendant knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity; and (4) the defendant acted with any of four enumerated intents.[8] Section 1957 similarly requires that a defendant had knowledge that the transaction involves the proceeds of specified unlawful activity, but replaces the second 'four intents' requirement with a requirement that the transaction involve a financial institution and at least US$10,000.

In part because of the challenge of meeting the criminal burden of proof (i.e., beyond a reasonable doubt) that property involved in a transaction represents the proceeds of specified unlawful activity, especially in the context of international trade, the DOJ brings charges under Sections 1956 and 1957 relatively infrequently in TBML cases. Rather than a criminal action, the DOJ can seek civil forfeiture under US Code Title 18, Section 981 of property involved in a violation of Section 1956 or 1957 or other specified unlawful activity, or traceable to the property. Although a civil forfeiture action similarly requires proof of specified unlawful activity and a nexus between that activity and the property at issue, the government faces a lower burden of proof in the forfeiture context; the government can seize property if it has probable cause that it was involved in specified unlawful activity and must ultimately prove that the property is subject to forfeiture by a preponderance of evidence. Moreover, because civil forfeiture cases are *in rem* actions, the government need not prove that any specific defendant committed a crime.

Beyond the DOJ, several US government agencies enforce laws and related regulations that target aspects of TBML. In particular, the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) enforces the Bank Secrecy Act (BSA) and the relevant provisions of the Uniting and Strengthening

8 The four intents are (1) the intent to promote the carrying on of specified unlawful activity, (2) the intent to engage in tax evasion or tax fraud, (3) knowledge that the transaction was designed to conceal or disguise the nature, location, source, ownership or control of proceeds of specified unlawful activity, or (4) knowledge that the transaction was designed to avoid a transaction reporting requirement.

America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, together requiring financial institutions in the United States to assist US government agencies to detect and prevent money laundering, for example, by establishing risk-based procedures for verifying customers' identities.[9]

These agencies work together, and with other law enforcement agencies such as the Federal Bureau of Investigation, Drug Enforcement Agency, the Department of Treasury's Office of Foreign Assets Control (OFAC), the Department of Homeland Security – in particular its TBML-focused Trade Transparency Unit – Customs and Border Protection and the Internal Revenue Service (IRS), to detect, investigate and enforce TBML-related laws and regulations against not only those bad actors central to TBML but also merchants, financial institutions and others providing professional services that are complicit, often unknowingly, in the schemes.[10]

Recent enforcement actions

Recent enforcement actions highlight the types of TBML that the DOJ and other US regulators seek to disrupt, as well as how third parties can be swept up in such schemes.

In November 2018, an interagency force led by the DOJ, the US Immigration and Customers Enforcement and the IRS alleged that an individual named Enayatullah Khwaja and six other co-conspirators perpetrated an international

9 8 U.S.C § 1701; Comply Advantage, 'USA Patriot Act: BSA Compliance and Section 314' (https://complyadvantage.com/insights/usa-patriot-act/ (accessed 11 July 2023)). The general purview and capabilities of the US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) can be found at https://www.fincen.gov/what-we-do (accessed 11 July 2023); Federal Deposit Insurance Corporation, 'Customer Identification Program' (February 2021) (https://www.fdic.gov/news/financial-institution-letters/2021/fil21012b.pdf (accessed 11 July 2023)).

10 The GAO Report provides a thorough explanation of both the interplay between US government agencies and US cooperation with other nations' law enforcement and financial institutions. See also 'National Money Laundering Assessment' (2018) (https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf (accessed 11 July 2023)); and John Cassera's talk to the Drug Enforcement Administration on the importance of trade-based money laundering in the future (28 February 2013) (https://museum.dea.gov/sites/default/files/2021-09/Trade-Based%20Money%20Laundering%2002282013--Accessible.pdf (accessed 11 July 2023)).

money laundering scheme.[11] Each of the defendants owned or were employed by family-run import-export businesses with offices in New York and Miami. The indictment alleged that the defendants accepted bulk cash deliveries from drug dealers and other criminals based in South America and the United States. The defendants allegedly obscured the illicit cash transfers through mobile phone sales and exports. Some transactions involved mobile phone sales and some were fabricated. A federal agent working on the case noted that it represented 'an international money laundering scheme relying on the complexities of global trade, and the use of [the defendant's] businesses here in New York and in Florida, to launder millions of dollars for transnational drug traffickers'.[12]

Nearly five years later, in April 2023, FinCEN relied in part on the *Khwaja* indictment to obtain its first-ever enforcement action against a trust company. According to the consent decree, Kingdom Trust Company (Kingdom Trust), chartered in South Dakota, had, among other things, processed transactions involving two of the mobile phone businesses identified in the *Khwaja* indictment.[13] Kingdom Trust's customer alleged that it was in the financial services industry, but FinCEN pointed out that that conflicted with the customer sending more than 150 transactions to beneficiaries allegedly in the mobile phone business, based in Miami with minimal to no online presence. FinCEN did not allege that Kingdom Trust was intentionally involved in the purported *Khwaja* scheme but concluded that Kingdom Trust's failure to detect and report this suspicious

11 Indictment, *United States v. Khwaja*, No. CR 18 607 (E.D.N.Y. Nov. 7, 2018) (https://www.justice.gov/usao-edny/press-release/file/1111661/download (accessed 11 July 2023)); US Immigration and Customs Enforcement, press release, '7 charged with laundering drug trafficking proceeds between US, South America' (18 November 2018) (https://www.ice.gov/news/releases/7-charged-laundering-drug-trafficking-proceeds-between-us-south-america (accessed 11 July 2023)).

12 US Attorney's Office for the Eastern District of New York (EDNY), press release, 'Seven Owners and Employees of Import-Export Companies Arrested for Conspiracy to Launder Drug Trafficking Proceeds and Related Crimes' (15 November 2018) (https://www.justice.gov/usao-edny/pr/seven-owners-and-employees-import-export-companies-arrested-conspiracy-launder-drug (accessed 11 July 2023)).

13 Consent Order Imposing Civil Money Penalty, *In re Kingdom Trust Co.* (April 2023) (https://www.fincen.gov/sites/default/files/shared/FinCEN_KTC_Consent%20Order_FINAL_508_042523.pdf (accessed 11 July 2023)).

activity 'may have caused substantial harm to the US financial system'.[14] Under the consent order, Kingdom Trust agreed to pay a US$1.5 million civil money penalty, admitting that it maintained an underdeveloped compliance programme and, as such, failed to both accurately and timely report suspicious activity by its customers.[15]

TBML also often utilises black market currency exchanges, such as the Black Market Peso Exchange in Colombia. As described by FinCEN, the complex scheme traditionally involves drug cartels selling US currency to black market peso exchangers in Colombia. Those exchangers place the money in US bank accounts and complete the scheme by selling monetary instruments that draw from those same bank accounts to Colombian importers for the purchase of foreign goods.[16]

In a recent case, a set of defendants allegedly perpetrated such a scheme by laundering millions of dollars derived from illicit drug sales through purported perfume sales. The defendants moved large amounts of cash (sometimes protected in heat-sealed packs, hidden in cereal boxes or kept as loose currency) using cars, buses and planes from various locations across Mexico and the United States to Laredo, Texas. Once in Laredo, the defendants brought the cash to various perfume stores. The perfume store owners then accepted the cash and shipped back perfume to Mexico, where it was converted into pesos for the traffickers moving drugs into the United States. The perfume store owners continued to participate in the scheme even after receiving warnings that the money involved was drug money; the owners also neglected to file the federal forms required when a business receives more than US$10,000 in cash. In February 2019, a

14 id.

15 US Department of the Treasury, FinCEN, press release, 'FinCEN Assesses $1.5 Million Civil Money Penalty Against Kingdom Trust Company for Violations of the Bank Secrecy Act' (26 April 2023) (https://www.fincen.gov/news/news-releases/fincen-assesses-15-million-civil-money-penalty-against-kingdom-trust-company (accessed 11 July 2023)).

16 FinCEN Advisory (November 1997) (https://www.fincen.gov/sites/default/files/advisory/advisu9.pdf (accessed 11 July 2023)).

jury found six defendants guilty of money laundering and related conspiracy charges after a five-week trial; one other defendant pleaded guilty to conspiracy to launder money.[17]

Another example arose in July 2022, when a federal grand jury indicted seven individuals for a wide-ranging set of drug trafficking-related money laundering (and other) violations. The defendants allegedly ran a money laundering ring that started in a family-owned restaurant in Boston's Chinatown. The DOJ claimed that the defendants engaged in off-the-books transactions in which they accepted illicit drug proceeds denominated in Chinese yuan and then sold the proceeds at a discounted exchange rate. Along with this classic form of money laundering, the defendants allegedly engaged in a 'sophisticated' TBML scheme, through which they stole or fabricated gift cards that they used to purchase thousands of Apple products. The defendants then shipped those products to Dubai and other international locations, receiving tens of millions of dollars in exchange.[18]

TBML, sanctions evasion and terrorist financing

As these examples demonstrate, TBML often arises in the context of illicit drug trading. Criminals also exploit international trade to engage in two other, often related violations: sanctions evasion and terrorist financing.

For background, the primary authority relating to US sanctions enforcement is the International Emergency Economic Powers Act (IEEPA)[19] and its implementing regulations, which grant the US President broad authority to impose economic sanctions during times of national emergency. Under IEEPA, OFAC administers and enforces economic and trade sanctions relating to non-US

17 US Department of Justice, press release 19-111, 'Six Convicted for Roles in Multi-Million Dollar Black Market Peso Exchange Money-Laundering Scheme' (12 February 2019) (https://www.justice.gov/opa/pr/six-convicted-roles-multi-million-dollar-black-market-peso-exchange-money-laundering-scheme (accessed 11 July 2023)); US Department of the Treasury, FinCEN, press release, 'FinCEN Recognizes Law Enforcement Cases Significantly Impacted by Bank Secrecy Act Filings' (19 May 2020) (https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act (accessed 11 July 2023)); see also *United States v. Gudipati*, No. 19-40524, 2021 WL 3744908, at *1 (5th Cir. Aug. 24, 2021).

18 US Attorney's Office (District of Massachusetts), press release, 'Eight Indicted in Money Laundering Ring' (29 July 2022) (https://www.justice.gov/usao-ma/pr/eight-indicted-money-laundering-ring (accessed 11 July 2023)).

19 50 U.S.C. ch. 35 § 1701, et seq.

countries, entities and individuals involved in various activities that threaten US national security, including terrorism.[20] These sanctions restrict US persons' involvement in certain financial transactions, trade and other economic activities.

In the context of terrorist financing, under US Code Title 18, Section 2339B,[21] it is illegal to provide material support or resources to designated foreign terrorist organisations. The term 'material support' encompasses diverse forms of assistance, including financial aid, goods, services and training. This statute aims to disrupt the financial networks of terrorist organisations by targeting individuals or entities involved in providing support, including those engaged in TBML schemes that facilitate the movement of funds for terrorist activities.

In using TBML techniques to circumvent sanctions or finance terrorist organisations, criminals exploit gaps or inconsistencies in international trade activities.[22] As with TBML more generally, exploitation can take the form of fraudulent invoicing, manipulation of shipping documents, or misrepresentation of goods to hide their true origin or destination.

Recent enforcement actions provide insight into how TBML interacts with sanctions evasion and terrorist financing.

In April 2023, the DOJ indicted Nazem Ahmad, a dual Belgian-Lebanese citizen who was sanctioned by OFAC in 2019 for acting as a financier for Hezbollah, alleging that he 'relied on a complex web of business entities to obtain valuable artwork from US artists and art galleries and to secure US-based diamond-grading services all while hiding Ahmad's involvement in and benefit

20 See US Department of the Treasury, Office of Foreign Assets Control, 'About OFAC' (https://ofac.treasury.gov/about-ofac (accessed 11 July 2023)); see also Thomas Reuters, 'OFAC Sanctions – A primer for in-house counsel' (10 April 2023) (https://legal.thomsonreuters.com/blog/ofac-sanctions-a-primer-for-in-house-counsel/ (accessed 11 July 2023)).

21 US Department of Justice, 'Providing Material Support to Designated Terrorist Organizations (Fundraising)' in Criminal Resource Manual (2020) (https://www.justice.gov/archives/jm/criminal-resource-manual-16-providing-material-support-designated-terrorist-organizations (accessed 11 July 2023)).

22 See, e.g., Raymond W Baker, 'The Biggest Loophole in the Free-Market System', Brookings Institution (1 September 1999) (https://www.brookings.edu/wp-content/uploads/2016/06/baker.pdf (accessed 11 July 2023)).

from these activities'.[23] In total, Ahmad's scheme involved financial transactions worth more than US$400 million, largely based on the sales of artwork and diamonds.[24]

Ahmad's network – based in Britain, Belgium, Hong Kong, Lebanon, the United Arab Emirates (UAE), South Africa, Angola, Ivory Coast and the Democratic Republic of the Congo – allegedly relied on different unlawful arrangements, including TBML techniques, to evade sanctions and support sales of artwork and diamonds across the world; for example, the scheme allegedly involved undervaluing certain goods in documentation submitted to US Customs. Certain involved parties falsely engineered certificates to manipulate diamond prices. The scheme also relied on front companies, fraudulent paperwork and obscuring the value of items to avoid import taxes.[25]

After uncovering the scheme, OFAC sanctioned 52 individuals and entities. Under Secretary of the Treasury for Terrorism and Financial Intelligence Brian E Nelson stated, in announcing the sanctions targeting those involved in the scheme: 'Luxury good market participants should be attentive to these potential tactics and schemes, which allow terrorist financiers, money launderers, and sanctions evaders to launder illicit proceeds through the purchase and consignment of luxury goods.'[26] The DOJ has charged Ahmad and eight co-defendants with conspiring to defraud the United States and foreign governments, conspiring to evade US sanctions and customs laws, and money laundering, among other offences; although one defendant has been arrested, the others (including Ahmad)

23 See US Attorney's Office (EDNY), press release, 'OFAC-Designated Hizballah Financier and Eight Associates Charged with Multiple Crimes Arising Out of Scheme to Evade Terrorism-Related Sanctions' (18 April 2023) (https://www.justice.gov/usao-edny/pr/ofac-designated-hizballah-financier-and-eight-associates-charged-multiple-crimes (accessed 11 July 2023).

24 See US Department of the Treasury, press release, 'Treasury Disrupts International Money Laundering and Sanctions Evasion Network Supporting Hizballah Financier' (18 April 2023) (https://home.treasury.gov/news/press-releases/jy1422 (accessed 11 July 2023).

25 See id.

26 id.

remain at large.[27] As is standard in TBML cases, the government obtained seizure warrants in connection with these charges for a diamond ring, cash, artwork and other assets collectively valued at millions of dollars.[28]

A long-running case involving Halkbank (a banking entity owned by the Turkish government), certain of its executives and other alleged co-conspirators provides another example of the use of TBML to gain access to the US financial system in violation of sanctions. According to the DOJ, the defendants participated in an elaborate multi-year scheme that used a network of money services businesses and front companies in Turkey and the UAE to use the proceeds of sales of Iranian oil to purchase gold for the benefit of the Government of Iran. Gold, and other fine metals, is a common medium of exchange in TBML schemes. The defendants here allegedly transferred proceeds from Iranian oil sales to exchange houses and front companies run by one of the defendants. Their conspirators used those proceeds to purchase gold in Turkey. They would then transport that gold out of Turkey and exchange it for cash to either return to Iran or use in other transactions for the benefit of persons in Iran. The conspirators also falsified documentation to falsely suggest that they returned the gold to Iran, rather than selling it for cash outside Turkey, involving US financial institutions in these activities in violation of then-applicable sanctions.

When the United States further restricted the relevant oil-related Iran sanctions, the defendants manipulated transactions involving the proceeds of Iranian oil to falsely appear to involve the purchase of food and medicine, authorised under US sanctions under certain conditions; for example, when the involved banks requested bills of lading to demonstrate the humanitarian aid involved in the shipments, a defendant claimed that the 'small, five-ton wooden ships' transporting the goods could not provide bills of lading, and at other times provided fraudulent documentation.[29]

---

27 See US Attorney's Office (EDNY), press release (op. cit. note 22); see also Karen Zraick, 'Art Collector Who Financed Hezbollah Evaded Sanctions, Prosecutors Say', *The New York Times* (18 April 2023) ('His extensive art collection at the time included works by Picasso and Warhol, and many were displayed in his Beirut penthouse') (https://www.nytimes.com/2023/04/18/nyregion/art-dealer-sanctions-hezbollah.html (accessed 11 July 2023)).

28 See US Attorney's Office (EDNY), press release (op. cit. note 22).

29 See Indictment, *United States v. Zarrab*, No. S4 15 Cr. 867 (RMB) (S.D.N.Y. Mar. 30, 2016) (https://www.justice.gov/usao-sdny/press-release/file/994976/download (accessed 11 July 2023)).

In 2018, Mehmet Atilla, a former Halkbank executive and one of the defendants allegedly involved in the conspiracy, was found guilty by a jury of conspiring to violate US sanctions relating to Iran.[30] Cases against Halkbank itself and certain other defendants remain pending.

Collectively, these cases establish that those looking to evade sanctions or finance terrorists often do so by relying on TBML techniques, including by manipulating legitimate trade routes for illicit purposes.

Risks and vulnerabilities with trade finance

Merchants, exporters, freight forwarders and the like are not the only parties that may be liable for involvement in TBML: financial institutions also face exposure when they support and finance transactions involving international trade (i.e., engage in trade finance). Trade finance refers to the financial activities and products that facilitate international trade, including related funding, risk mitigation and settlement processes.

Financial institutions may unwittingly support TBML when engaging in trade finance because of, among other factors, the large numbers of involved parties (such as exporters, importers, banks, shipping companies, freight forwarders, agents, insurers and customs agencies), the presence of different regulators and jurisdictions involved at different parts of the process, limited visibility by financial institutions into shipping and other trade documentation, and the widespread use of fraudulent documentation in trade finance. These factors allow TBML to pose a risk to the trade finance space as it does to industries engaged in international trade more broadly.[31]

In 2018, a court in the Southern District of California held that a California-based bank had conspired to impair, impede and obstruct the Department of the Treasury's Office of the Comptroller of the Currency by

30 See US Attorney's Office for the Southern District of New York, press release, 'Turkish Banker Mehmet Hakan Atilla Sentenced to 32 Months for Conspiring to Violate U.S. Sanctions Against Iran and Other Offenses' (16 May 2018) (https://www.justice.gov/usao-sdny/pr/turkish-banker-mehmet-hakan-atilla-sentenced-32-months-conspiring-violate-us-sanctions (accessed 11 July 2023).

31 See GAO, 'Countering Illicit Finance and Trade: Better Information Sharing and Collaboration Needed to Combat Trade-Based Money Laundering' (https://www.gao.gov/assets/gao-22-447.pdf (accessed 11 July 2023).

concealing deficiencies in its anti-money laundering programme.[32] The bank forfeited more than US$368 million for having processed transactions 'consistent with illegal activity such as trade-based money laundering, bulk cash smuggling, structuring, and the black market peso exchange'.[33]

TBML red flags

Businesses involved in international trade should be on the lookout for red flags indicating potential risks or illicit activities in the context of international trade and related transactions. Effective compliance programmes designed to identify red flags can allow organisations to quickly address potential compliance issues and assess the legitimacy of their customers or counterparties to avoid inadvertently facilitating TBML and potentially creating criminal or civil liability.

A number of red flags may suggest a heightened risk of TBML in connection with a given shipment or transaction.[34]

- *Touchpoints to higher-risk jurisdictions*: Certain countries or regions present a relatively high risk of money laundering, terrorist financing or other illicit activities. Any touchpoints to these jurisdictions may raise red flags even if no party is located in that jurisdiction; for example, if a party often routes its shipments through countries known to have weak regulatory frameworks or minimal enforcement of illicit activities.
- *Needlessly complex transaction structures*: Transaction structures that seem unnecessarily complex, convoluted or serve no apparent legitimate purpose might seek to obscure the true nature of a transaction.
- *Payments directed to or from an unrelated third party*: If a party insists on issuing a payment to a seemingly unrelated third party, particularly one not involved in or with no apparent connection to the transaction, it can be a red flag for potential money laundering or fraud. Similarly, payments for goods or services from one or more third parties with no apparent relationship to the purchaser can be a red flag.

---

32 See US Attorney's Office for the Southern District of California, 'Bank Sentenced for Obstructing Regulators, Forfeits $368 Million for Concealing Anti-Money Laundering Failures' (18 May 2018) (https://www.justice.gov/usao-sdca/pr/bank-sentenced-obstructing-regulators-forfeits-368-million-concealing-anti-money (accessed 11 July 2023).

33 id.

34 This is a not an exhaustive list. More indicators can be found in, for example, the Federal Financial Institutions Examination Council's BSA/AML Examination Manual, Appendix F (https://bsaaml.ffiec.gov/manual/Appendices/07 (accessed 11 July 2023)).

- *Shipments involving products inconsistent with the identified business*: A party may raise suspicions by placing an order or shipping items seemingly unrelated or inconsistent with the party's line of business; for example, a clothing retailer suddenly placing a large order for high-tech networking equipment. Shipments involving items subject to especially high restrictions, such as weapons, controlled technologies or embargoed goods, may especially raise compliance concerns.
- *Over- or under-pricing of goods and services*: Significant deviations from market prices or inconsistent pricing patterns, such as unusually low prices or inflated invoices, may indicate attempts to manipulate financial transactions or disguise the true value of goods and services.
- *Irregular shipping documentation*: Shipping documentation, including purchase orders, letters of credit, bills of lading and other documents, that is incomplete, inconsistent or otherwise irregular can be a red flag; for example, frequent or substantial amendments to shipping documentation, especially those involving changes to the beneficiary or payment location, without reasonable explanations can suggest attempts to manipulate or abuse the transaction. Discrepancies between the actual shipment details, such as the destination or description of goods, and the information in shipping documentation may raise suspicions about the authenticity or legitimacy of the transaction.

The presence of one or more red flags does not automatically imply wrongdoing but should prompt additional scrutiny and due diligence of the transaction.

Risk mitigation

Certain parties – in particular, financial institutions – are legally obliged within certain jurisdictions to implement compliance measures tailored to identifying suspicious transactions, including those involving TBML. Even if no such obligation exists, adopting and maintaining robust compliance programmes designed to detect, investigate and internally raise red flags of TBML and related suspicious activities can help to ensure compliance with applicable laws and regulations.

Due diligence is the crucial process to assess and mitigate risks associated with international trade transactions. Evaluating the financial, commercial and legal aspects of a trade deal allows a party to identify red flags suggesting a transaction may relate to TBML. Some of the best practices for conducting due diligence to avoid incidental involvement in TBML – or other illicit activities – include:

- *know your customer*: perform thorough procedures to verify the legal existence, identity and credibility of the buyer, seller and any intermediaries involved. This involves the collection of corporate information, including company

details, financial statements, legal documentation and track records.[35] Screening parties against sanctions-related denied parties lists mitigates both TBML and related sanctions and terrorist financing risks;

- *transaction review*: review the terms and conditions of the transaction, including the contract, purchase orders, invoices, shipping documents and payment terms. This includes verifying the accuracy and consistency of information provided;
- *financial analysis*: conduct a comprehensive financial analysis of the parties involved, focusing on their liquidity, solvency, profitability and financial stability. This may include assessing involved parties' ability to fulfil payment obligations, collateral valuation and potential exposure to financial risks;[36]
- *legal and regulatory compliance*: evaluate any legal or regulatory restrictions that may affect the transaction, and ensure compliance with applicable laws and regulations, including sanctions;
- *country risk assessment*: evaluate any specific political, economic and legal risks associated with the countries involved in the transaction. Relevant factors include stability, currency risks, legal framework, corruption levels and trade restrictions that could affect the transaction;[37]
- *industry and market analysis*: understand the industry and market dynamics relevant to the trade transaction by, for example, analysing market conditions, the competitive landscape and the parties' reputations and position within their respective industries; and
- *risk mitigation techniques*: identify and implement appropriate risk mitigation techniques. These can include obtaining guarantees or letters of credit, using insurance policies or involving reputable third-party service providers.[38]

---

35 The Society for Worldwide Interbank Financial Telecommunication (Swift) has a thorough exploration of the topic: see 'What is KYC?' (https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/meaning-kyc (accessed11 July 2023)).

36 See Anna M Costello, 'The Value of Collateral in Trade Finance', *Journal of Financial Economics* (10 July 2018) (https://ssrn.com/abstract=3211542 (accessed11 July 2023)).

37 Country commercial guides are available via the International Trade Administration website (https://www.trade.gov/country-commercial-guides (accessed11 July 2023)).

38 Ernst & Young has further discussion in 'How technology is reducing trade finance risk and compliance costs' (https://www.ey.com/en_gl/banking-capital-markets/how-technology-is-reducing-trade-finance-risk-and-compliance-costs (accessed 11 July 2023)); Patrick Craig et al., 'Why banks should transform trade finance controls' (11 January 2022) (https://www.ey.com/en_gl/financial-services-emeia/transforming-banks-trade-finance-controls (accessed 11 July 2023)).

Persistent monitoring and reporting is essential to ensuring an effective compliance programme, beyond these transaction-specific actions. This involves establishing mechanisms to monitor continuing transactions and identify any red flags or deviations from the agreed terms, regularly reviewing the financial and operational performance of the parties involved, and maintaining clear and concise internal reporting mechanisms to ensure transparency and accountability.

Appropriate due diligence should be tailored to a specific transaction and its unique risk factors. Regularly updating and refining due diligence processes based on market conditions, regulatory changes and shifting risks is essential to ensure risk mitigation relating to TBML.

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-255-0

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Accuracy

Charles River Associates

FTI Consulting Inc

Herbert Smith Freehills

Latham & Watkins LLP

Morgan, Lewis & Bockius LLP

Morgan Lewis Stamford LLC

Orrick, Herrington & Sutcliffe LLP

Sullivan & Cromwell LLP

Venable LLP

Von Wobeser y Sierra, SC

Willkie Farr & Gallagher LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

The Guide to Anti-Money Laundering is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell our readers everything they need to know about all that matters in their chosen professional niche.

Thanks to GIR's position at the heart of the investigations community, we often spot gaps in the literature. *The Guide to Anti-Money Laundering* is a good example. For, despite a greater effort than ever to prosecute and eliminate money laundering by targeting financial gatekeepers, there is still no systematic work tying together all the trends in the area. This guide addresses that.

Its title is a little misleading. In fact, it covers both sides of the coin – trends in both the enforcement of money laundering laws (comprising Part I) and the operation of anti-money laundering regimes and the exigencies of compliance (Part II). Incorporating all of that in the title would have made it a little long (and slightly alarming: '*A Guide to Money Laundering . . .*' sounds quite wrong).

The guide is part of GIR's steadily growing technical library. This began six years ago with the first appearance of the revered GIR *Practitioner's Guide to Global Investigations*. *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to do or think about at every stage. Since then, we have published a series of volumes that go into more detail than is possible in *The Practitioner's Guide* about some of the specifics, including guides to sanctions, enforcement of securities laws, compliance and monitorships. I urge you to get copies of them all (they are available free of charge as PDFs and e-books on our website - www.globalinvestigationsreview.com).

Last, I would like to thank our external editor, Sharon Cohen Levin, for helping to shape our lumpier initial vision, and all the authors and my colleagues for the elan with which they have brought the guide to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher, GIR
August 2023