Identifying and interdicting sanctions risk in global transshipment and intermediary points

EY
Building a better working world

A series of actions by the Office of Foreign Assets Control (OFAC) throughout 2016 and into 2017, including multiple enforcement actions and designations, highlighted the sanctions risk posed by transshipment and intermediary points — geographic and financial hubs for goods and payments ultimately destined to sanctioned jurisdictions. Patterns in regulatory focus are typically established through years of guidance, enforcement actions and consistent public messaging. It is notable that many of OFAC's 2016 actions highlighted a common theme: the shipment of goods and processing of payments to sanctioned jurisdictions through third-party countries that themselves are not sanctioned. Some of these enforcement actions dealing with transshipment and intermediary risk were levied against financial institutions, which regulators argue "should have known" that they were facilitating prohibited activity.[1]

A variety of sources consistently demonstrate that sanctioned entities gain access to the international financial system through third-party intermediaries and non-sanctioned countries. Financial institutions employ a range of controls to root out and prevent activity directly citing sanctioned entities or jurisdictions. However, the use of intermediary and transshipment points ("intermediary points") creates an additional layer of obfuscation that facilitates transactions to, or trade involving, sanctioned entities and jurisdictions. Similar to the classic money laundering maxim — funds are first placed, then layered and finally integrated into the financial system — the use of an additional layer for trade or transactions can facilitate access to the international financial system for sanctioned entities or jurisdictions.[2,3,4]

Companies and individuals seeking to circumvent sanctions are aware of financial institutions' controls, as evidenced by their constantly evolving behavior, changes in naming convention, resubmitted payments, use of intermediary points and other evasive tactics. Financial institutions already have obligations to identify and interdict prohibited activity and should be enhancing compliance controls to stay ahead of illicit actors' intentions. This article outlines potential enhancements related to mitigate intermediary risk.

Financial or trade activity passing through a non-sanctioned country should not be considered absent of sanctions risk.

[1] EY analysis of OFAC civil penalties and enforcement actions which resulted in a monetary penalty between 2013 and 2017.

[2] OFAC civil penalties and enforcement information, 2013 – 2017, https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx, accessed July 2017.

[3] United Nations North Korea Panel of Experts, *"Report of the Panel of Experts established pursuant to resolution 1874"*, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150, accessed July 2017.

[4] United States of America v. Reza Zarrab, June 2017, 15 CRIM 867, accessed June 2017.

What makes transshipment and intermediary points high-risk for sanctions compliance?

Intermediary points provide an alternative channel for gaining access into a sanctioned jurisdiction or for those based in a sanctioned jurisdiction to gain access to the international financial system. Rather than directly interacting with a sanctioned jurisdiction, for example, activity can pass through these intermediary points. Several interrelated factors contribute to intermediary and transshipment point risk.

An added layer of legitimacy

Many banks maintain a methodology for rating the risk associated with foreign jurisdictions. A list of high-risk countries feeds into client risk ratings, transaction monitoring scenarios and other controls. Personnel are trained to assess and treat a transaction to a low-risk country differently from one to a high-risk country. While some intermediary points are based in traditionally high-risk countries, our review of OFAC enforcement actions, law enforcement cases and other open sources suggests traditionally low-risk countries also often serve as intermediary points. Passage of trade or transactions through lower-risk countries provides a layer of legitimacy to the activity, leading to potentially less scrutiny by compliance personnel and business lines. Whereas the involvement of a third party in a high-risk country greatly increases the perceived risk of a transaction for anti-money laundering compliance, the involvement of a non-sanctioned jurisdiction often decreases the perceived risk of activity for sanctions compliance.

A lack of data increases the difficulty of sanctions compliance efforts

For financial institutions, the risk associated with intermediary points can be condensed into a key question: if a transaction, trade finance activity or other payment does not explicitly detail sanctions exposure, how can financial institutions still detect and stop activity ultimately destined for a sanctioned party or country? In a June 2015 advisory, OFAC illustrated this risk factor by noting that transactions and trade access to Crimea, a region subject to comprehensive US sanctions, was facilitated by the removal of keywords in payment messages and the use of intermediaries in third-party countries.[5] Some trade or transaction activity passing through intermediary points is facilitated by malicious activity specifically meant to circumvent sanctions, including through the "stripping" of key payment information. However, other activity to intermediary points never mentions a sanctioned entity or jurisdiction, which negates the ability to use traditional sanctions screening tools to interdict the activity.

[5] *Crimea Sanctions Advisory*, "Obfuscation of Critical Information in Financial and Trade Transactions Involving the Crimea Region of Ukraine," Office of Foreign Assets Control, 30 July 2015, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/crimea_advisory.pdf, accessed May 2017.

A difference in sanctions compliance obligations

A major risk factor associated with foreign jurisdictions includes financial institutions' differing standards for anti-money laundering compliance. The same is true for sanctions compliance. A 2015 report issued by the Financial Action Task Force noted that many countries continue to struggle with implementing the global standard-setting body's recommendation on targeted financial sanctions, which directly impacts local banks' sanctions screening obligations.[6] Some intermediary points are located in jurisdictions that have drastically different anti-money laundering, counter terrorist financing or sanctions compliance standards than those in the United States. Their permissive environment for trade and transactions involving sanctioned jurisdictions is often not malicious but rather the result of varying standards and rules.

A similar level of responsibility

OFAC's standard for sanctions compliance is often cited as "known or should have known."[7,8] Enforcement actions and the agency's guidelines show how financial institutions, as much as resellers of goods destined for sanctioned jurisdictions, are held responsible for processing activity that ultimately benefits a sanctioned entity or jurisdiction. Even if a transaction does not explicitly cite exposure to a sanctioned entity, but a processing financial institution could have obtained information to understand that a sanctioned entity was involved, that activity is prohibited and may expose the bank to regulatory or enforcement action, depending on the severity and a variety of other factors. Since 2012, approximately 35% of OFAC's public civil enforcement actions have highlighted that goods or transactions eventually bound for a sanctioned jurisdiction first pass through an "intermediary or transshipment point," according to EY analysis of those actions.

---

[6] *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)*, Financial Action Task Force (FATF), 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf, accessed May 2017.

[7] "CISADA: The New U.S. Sanctions on Iran," *U.S. Department of the Treasury website*, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/CISADA_english.pdf, accessed May 2017.

[8] "ENFORCEMENT INFORMATION FOR FEBRUARY 25, 2016: Halliburton Atlantic Limited and Halliburton Overseas Limited Settle Potential Civil Liability for Alleged Violations of the Cuban Assets Control Regulations," *U.S. Department of the Treasury website*, 2016, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20160225_Halliburton.pdf, accessed May 2017.

How can banks interdict prohibited activity passing through transshipment and intermediary points?

A number of control enhancements can lead financial institutions to better understand their exposure to potentially prohibited activity involving intermediary points and work to mitigate the risk associated with inadvertently facilitating activity on behalf of sanctioned entities or jurisdictions. Building a list of relevant intermediary points is a key first step. Financial institutions should review reliable public sources, enforcement actions and regulatory advisories to identify which intermediary points are most relevant and unique to their business.

Collect data on exposure to intermediary points

Once financial institutions understand what intermediary points apply most to their operating environment, they should take steps to understand the scope of their exposure. One way of doing this is through risk assessments specifically targeted to sanctions risk. Mature sanctions risk assessments collect a range of quantitative data on exposure to sanctions risk factors, including value and volume of transactions with high-risk countries. However, that data collection is rarely inclusive of more detailed information beyond the country-level view. Financial institutions may consider collecting quantitative data not only on which countries they sent or received money from, but also if any significant portion involved an intermediary point, or the number of clients operating in known intermediary points.

Analyze intermediary risk using internal intelligence

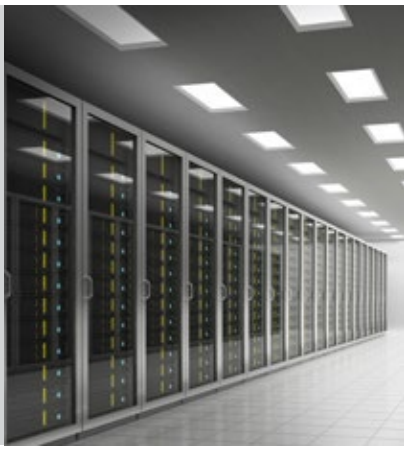
Banks' internal financial intelligence units are increasingly being used to identify unique money laundering risk, but those resources are often less focused on sanctions risk. Much like financial intelligence units use a range of internal payment data, customer data, external law enforcement and press reporting to proactively protect from emerging money laundering risks, banks can also analyze payment data, customer activity, blocked and rejected payments, voluntary self-disclosures, request for information responses, and other unique data to determine whether the risk of intermediary points is being mitigated.

Review the possibility of tiered screening

As noted above, the risk involving intermediary points is most pronounced when activity involving one of those cities, ports or regions does not explicitly mention a sanctioned entity or jurisdiction in a transaction or payment message. However, financial institutions may be able to use "tiered screening" to first identify exposure to an intermediary point and then the presence of specific keywords to generate an alert on that activity. The presence of the intermediary point or the keywords alone should not be used to produce alerts, as the enormous volume of false positives would be counterproductive, but the combination can yield valuable information on potential sanctions risk. These keywords can be gleaned from a variety of sourcing, including previous rejections, blocking actions and self-disclosures involving intermediary points.

Use all information available

Screening alert review analysts are typically trained to use a broad range of information to support their decision-making. Nevertheless, basic information sources, including the websites of companies involved in a transaction, often go untapped. A March 2016 US District Court decision underscored the extent of OFAC's "known or should have known" standard. The court noted that readily-available internet information could have been used to identify that goods destined for a transshipment point were ultimately destined for a sanctioned jurisdiction.[9] Separately, several online resources track the movement of maritime shipping vessels. Their travel to transshipment ports may be viewed as an increased first factor for potential prohibited activity, especially in the context of banks' trade finance business lines.



Review screening system performance on an ongoing basis

Ongoing tuning and calibration of sanctions screening systems, as well as the application of rigorous governance and change control procedures, must be viewed as key sanctions compliance controls. A strong screening system remains among the most effective and basic controls for overall sanctions compliance, including related to interdicting activity involving intermediary points. While a principal risk involving intermediary points is that no information is included in a payment message that a financial institution could use to interdict and review activity, some activity will always explicitly name a sanctioned entity or jurisdiction. Financial institutions should make sure that screening systems are accurately receiving data from upstream platforms and that current settings and tunings are appropriate for geographic, product and customer exposure, especially as the bank experiences growth.

Sanctions risk is often defined as direct exposure to embargoed jurisdictions or entities included on various sanctions lists. Debate around the ability to conduct activity with sanctioned entities is cut-and-dried: activity with entities on a sanctions list is prohibited (with few exceptions), and activity with entities not on a sanctions list is permitted. However, the risk associated with intermediary and transshipment points demonstrates how this interpretation of sanctions compliance obligations does not capture the full picture. Intermediary and transshipment points are a risk to financial institutions because they create a layer of obfuscation that complicates efforts to identify the ultimate purpose and beneficiaries and because banks in those areas have vastly different sanctions compliance obligations from banks in the United States and Europe. Without efforts to implement enhanced controls focused on intermediary and transshipment points, banks may fall behind in their compliance obligation to identify if activity is prohibited. Some of these enhancements are based on data collection — meant to help banks understand their exposure — while others are focused on interdiction, including through improvements to sanctions screening controls. By implementing a collection of both, financial institutions can better understand their exposure and interdict payments and trade activity that is ultimately destined for a sanctioned entity or jurisdiction.

[9] *Epsilon Electronics Inc. v. United States Department of the Treasury, Office of Foreign Assets Control, et al.*, 2016, https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2014cv2220-26, accessed May 2017.

Transshipment and intermediary risk: an illustrative case study involving Crimea, an OFAC-sanctioned jurisdiction*

* This case study is fictional. None of the names are based on real companies or experiences and were created for this article only.

Transshipment risk factors

step one

Distilling Powerfully Ltd

A South Africa-based manufacturer of industrial distillers used for wine production receives an order for six distillers.

Differing sanctions obligations

The illustrative South African business seeks trade finance support from a local bank related to the shipment of the distillers. The local bank's sanctions compliance obligations – in part set by the local regulatory agencies – does not consider Crimea as a sanctioned jurisdiction.

step two

European Bank, New York Branch

Serves as the clearing bank for the SWIFT** payment-related messages and CHIPS*** funds transfers. Third-party banks provide trade finance support for the activity.

Disparate information

While European Bank is asked to process the SWIFT MT202COV payment associated with the purchase of the distillers, it does not have direct access to the underlying trade finance documentation that would help it identify exposure to a sanctioned jurisdiction.

step three

May First Exporters LLC

An import/export firm based in a transshipment point located on the border with Crimea, a US-embargoed jurisdiction, is the initial recipient of the distillers and placed the order with Distilling Powerfully Ltd. The order was placed for a third-party customer.

Transshipment location

May First Exporters LLC is based in a port city on the border with Crimea. Over the past 18 months, OFAC has sanctioned numerous entities in this city, and reputable media reports indicated it is an entry point into Crimea.

step four

Bochki Vino LLC

A wine producer in Yalta, a city in Crimea, is the ultimate beneficiary of the distillers. Their involvement is stated in several of the invoices and trade finance documents.

Potential control enhancements

Keyword searches

European Bank's screening system did not create an alert for the payment messages associated with this activity, as the name of a sanctioned entity or sanctions jurisdiction was not present. Tiered screening for transshipment cities and other keywords (for example, "export") may have alerted the bank to request underlying trade finance documents from the third-party banks.

Financial intelligence analysis

Similar to how banks' financial intelligence units track emerging money laundering risks and trends, they can be used to understand how a financial institution is exposed to transshipment points. The involvement of an entity in a transshipment point may have raised the need for additional due diligence.

Due diligence

The website for May First Exporters LLC, while not available in English, clearly states that they export many goods to Crimea. Research into the website may have identified this risk factor.

** Society for Worldwide Interbank Financial Telecommunication

*** Clearing House Interbank Payments System

Contacts

EY is an industry leader in providing sanctions compliance, risk and technology advisory services to financial institutions, financial technology firms and other industries. To learn more about our experience, please reach out to any of the following subject-matter advisors:

Steve Beattie
Principal
Ernst & Young LLP
steven.beattie@ey.com

Jonathan Burke
Senior Manager
Ernst & Young LLP
jonathan.burke@ey.com

Brian Ferrell
Principal
Ernst & Young LLP
brian.ferrell@ey.com

Thomas Scazzafavo
Senior Manager
Ernst & Young LLP
thomas.scazzafavo@ey.com

Rob Mara
Principal
Ernst & Young LLP
robert.mara@ey.com

Kirill Meleshevich
Manager
Ernst & Young LLP
kirill.meleshevich@ey.com

Erin McAvoy
Principal
Ernst & Young LLP
erin.mcavoy@ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no: 04490-171US
1704-2259138
ED None

ey.com