FiveBy

POLICY ADVISORY

Sophisticated Sanctions Evasion Methodologies Require Human Touch

Executive Summary

The embargo the United States imposed on Crimea in response to Russia's 2014 annexation has resulted in the development of sophisticated sanctions evasion techniques by entities located there. Large multinational corporations face an especially significant risk when resellers—businesses and individuals that purchase and resell US products—provide these goods to customers in Crimea because of the sheer volume of sales and the number of reseller business partners with whom they engage. Through human-driven analysis, FiveBy has identified six common reseller evasion methods related to company registration, company leadership, activity mismatch, vague product descriptions, open tender bidding, and ambiguous address information used by entities in Crimea to illegally access US products and technologies.

Introduction

In December 2014, the Obama administration issued Executive Order (EO) 13685, prohibiting direct and indirect transactions in any goods, services, or technologies to and from Crimea. In response to the embargo, companies and government departments in Crimea began employing evasion methodologies to obtain business-critical US services and tools that they were unable to develop locally.

In 2015, the Treasury Department's Office of Foreign Assets Control (OFAC) warned about the obfuscation of references to Crimean locations in documentation involving the United States as an emerging sanctions evasion technique used by entities there. Entities located in Crimea would also omit the originator or beneficiary address in Society for Worldwide Interbank Financial Telecommunications (SWIFT) messages used by financial institutions to securely send and receive information and instructions for money transfers and other financial transactions.

In the past several years, Crimean entities have begun using more complex sanctions evasion methodologies that are difficult to detect through automated screening. OFAC over the past year penalized US companies, including Amazon and BitGo, for violating the Crimea embargo, demonstrating the regulatory and financial risks involved in relying heavily on automation to conduct due diligence on embargoed regions. Through research of Russian public tenders and government databases, FiveBy has detected and summarized several common forms of reseller evasion techniques that firms can use as a guide to avoid embargo violations.

Reseller Red Flags

1. Methodology: **Company is registered in Russia but selling primarily to customers in Crimea**
   Entities that want to conceal their operations in Crimea will provide a legitimate registration address in Russia; however, their primary geographical area of business is Crimea. Entities may use this strategy to evade detection by screening tools programmed to flag addresses in Crimea as well as evade basic due diligence.

INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM

Example: Reseller A is registered in Krasnodar, Russia. However, most of its government customers are located in Crimea.

Detection: Basic research will confirm that Reseller A is, in fact, registered at the given Russian address, but that it was registered just months after the United States imposed sanctions on Crimea—in and of itself a red flag. A more in-depth examination of Reseller A's government contracts using a Russian government database reveals that during the past year, 11 of this company's 15 government customers were in Crimea.

2. Methodology: **Company leaders oversee multiple companies reselling US products and technologies to entities in Crimea**
   Leaders or shareholders of a company that resells products into Crimea could use other companies in which they hold shares or leadership positions and that are located outside the embargoed region to evade sanctions.

   Example: Media reports show that Reseller B, registered in Moscow, has been reselling generators to entities in Crimea. The individual who owns and manages Reseller B also owns and manages Reseller C, which is registered at the same address in Moscow and which due diligence reveals also has government contracts for generators in Crimea.

   Detection: Checking the names of ultimate beneficial owners (UBOs) and general directors against sanctions lists and third-party databases will show if the individual is subject to sanctions but will not reveal whether the individual conducts business in Crimea. If a reseller does business with entities in Crimea, research into the business activities of entities owned or controlled by the same individuals should help provide insight into possible sanctions evasion.

3. Methodology: **Business activity registration mismatch**
   Although incongruous business activities may not be **directly** indicative of sanctions evasion, a mismatch of activities warrants additional investigation. A company reselling goods and services to entities in Crimea or other embargoed regions could indicate the use of a seemingly innocuous line of business in its registration documents to avoid scrutiny and obfuscate its business in embargoed regions.

   Example: Reseller D's main business activity is animal breeding, but all its government contracts in Crimea are for the provision of generators.

   Detection: Comparing the main registered business activity in official documents with the company's government contracts, as well as with the services advertised on its website, may provide insight into possible tactics to circumvent the embargo.

4. Methodology: **Vague descriptions of goods on government tenders**
   To avoid detection, firms that resell US goods to Crimea often will provide only vague descriptions of the goods they are reselling to Crimean companies, failing to mention specific brand names subject to the embargo.

Example: Reseller E, registered in Nizhny Novgorod, has a 2019 contract to provide US Brand X generators to a government entity in Crimea. Enhanced due diligence on Reseller E's business history reveals that this company also had a contract in 2018 for provision of "backup power sources" to a Crimean customer. Even though the 2018 contract does not specify Brand X generators as the item being provided, this contract indicates that the company has a history of reselling similar products to Crimea.

Detection: When a reseller has a tender in Crimea, especially for vaguely titled goods resembling branded goods it resells to non-embargoed regions, its reselling activities and government tenders should be closely monitored.

5. Methodology: **Bids on open tenders for US-branded products without obtaining a general license to resell goods to entities located in Crimea**

   Example: Individual Proprietor A has won a tender to provide generators to a Crimean institution, according to a Russian trade database. However, a reseller, which according to historical research, was reselling US-branded generators in Crimea, also bid on this tender, indicating the reseller's willingness to sell US goods and services to the embargoed region.

   Detection: Examine the historical business activities of entities bidding on tenders reselling US-branded products to Crimea and determine whether they are providing US goods or technologies to the embargoed region.

6. Methodology: **Ambiguous address**
   To avoid detection of Crimea operations, a company provides nonconclusive or incomplete address information about its customer.

   Example: Research on Reseller F, located in Moscow, could not determine whether this company was purchasing US goods and services and reselling them to an end customer in Crimea because the end customer failed to provide an address.

   Detection: When an entity provides incomplete address information about the location of its customers, examine their public tenders through a database that analyzes Russian tenders to determine whether the entity is reselling US-branded goods into Crimea without an applicable general license.

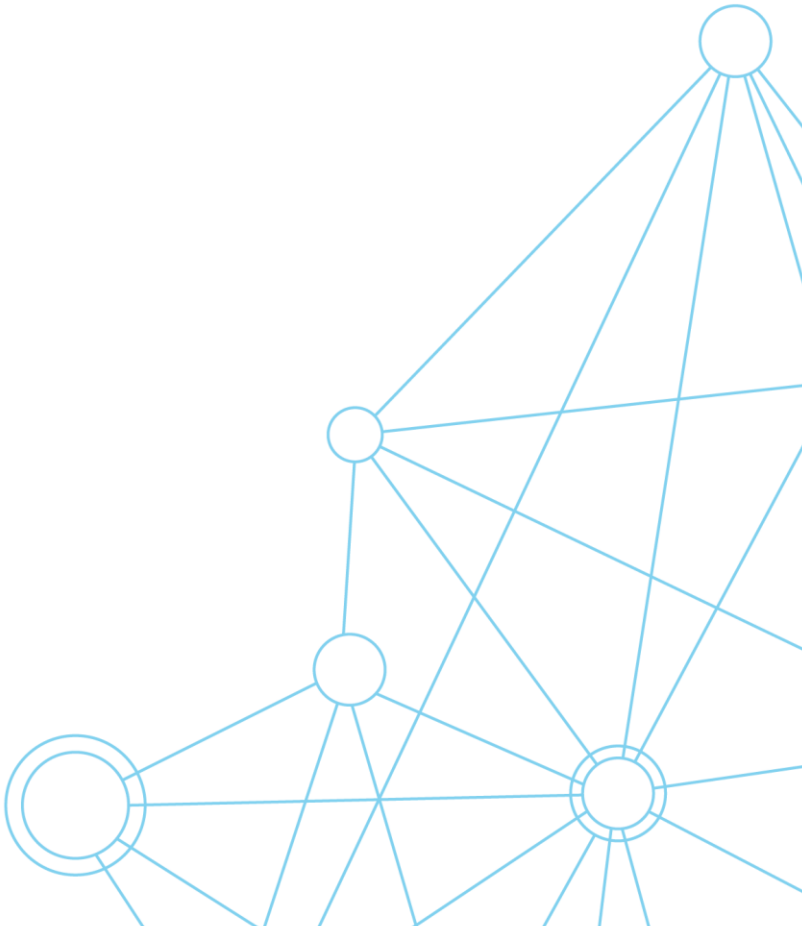
Conclusion

To best detect sanctions violations related to registration, company leadership, activity mismatch, vague product descriptions, open tender bidding, and ambiguous address information, firms need to conduct rigorous research into company business activities to supplement automated screening prior to authorizing a transaction. Subject matter experts with extensive regional and linguistic expertise are crucial to decipher and identify evasion practices. The penalty OFAC levied last year against Amazon for violating US sanctions by transacting in embargoed regions demonstrated that automated screening tools are not always sufficient to fully analyze all

transaction and customer data needed to ensure compliance. Through human-driven analysis, FiveBy detects sophisticated evasion techniques that automation often fails to detect.

FiveBy is a specialized risk intelligence services firm. We give you the insight you need to move faster and further with the confidence to transform your risks into opportunity. The opportunity to grow your profits, strengthen your brand, and exceed your customer expectations.

Our unique point of view brings together expertise spanning security, technology, data science, and business operations to connect your dots. By turning data into an enabler, FiveBy designs adaptable responses—whether to an ongoing incident or to implement preventive measures—tailored to your business needs and always with a human touch.



INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM