

Optimizing Sanctions Compliance: **Key** **Lessons from OFAC** **Enforcement Actions**

Ensuring Compliance in a Changing Global Landscape

Introduction 3

Timeline 6

2023 Sanctions Enforcement Actions

Case studies 8

Data Analysis 11

Risk Factors and Other Trends

Conclusion 15

Solutions and Recommendations

Introduction

What is OFAC and why is compliance important?

The Office of Foreign Assets Control, or OFAC, enforces US policy by prohibiting American companies from conducting business with sanctioned entities. The entities are listed on OFAC's Specially Designated Nationals (SDN) List, which is available and regularly updated on their website; many of the businesses and individuals are affiliated with Russia, Cuba, Syria, and Iran. All American entities, as well as those with American financial ties, must comply with the US sanctions regime. Since violations are considered strict liability offenses, companies can face criminal prosecution and/or financial penalties regardless of their intent or awareness. Non-compliance can lead to significant financial losses as well as damage to a company's reputation.

The expansion of globalization and trade over national borders has made it extremely difficult to monitor all company operations and ensure their compliance with US sanctions. However, entities face dire consequences when they ignore or subject these issues to compromise.

As demonstrated by the recent Microsoft settlement, violations of these laws can be extremely costly. While Microsoft may be equipped to handle losing over \$3 million, this is not the case for most companies. It should also be noted that Microsoft voluntarily disclosed their sanctions violations to the government; the settlement cost may have been much higher if they attempted to keep their misconduct a secret.

Complying with the constantly evolving sanctions landscape is a challenging task; the complexity of legal documents and the need to continuously monitor updates to sanctions and geographic regions require significant time and resources. The recent increase in sanctions against Russia, a global



Executive Summary

OFAC sanctions require compliance from all US-owned and affiliated entities. Violations are considered strict liability offenses for which companies (and people) can face criminal prosecution or financial penalties, regardless of awareness or intent. As the US sanctions regime continues to evolve and intensify, it is imperative that businesses develop a comprehensive understanding of compliance requirements to avoid reputational damage and costly government enforcement actions. Further investigation reveals potential solutions to this complex issue, such as proactive, preventative measures within company networks that can halt violations before they can occur.

business leader with long-standing relationships with many companies, has further complicated the compliance landscape.

To navigate this environment successfully while avoiding harsh penalties and reputational consequences, companies must adopt a comprehensive and proactive approach to mitigate risks and demonstrate due-diligence in their commitment to government regulations compliance. While creating an effective compliance strategy is a difficult task, it is certainly possible.



“Unless otherwise authorized or exempt, transactions by U.S. persons or in the United States are prohibited if they involve transferring, paying, exporting, withdrawing, or otherwise dealing in the property or interests in property of an entity or individual listed on OFAC’s SDN List.”

Office of Foreign Assets Control (OFAC)

Which countries and entities are currently sanctioned?

Currently, 38 OFAC sanctions programs are in effect. OFAC is the successor to the Office of Foreign Funds Control (the "FFC"), which played a major role in enforcing WWII's economic blockades of the Axis powers. OFAC was officially created in 1950, when the Korean War began and President Truman placed sanctions on China and North Korea. Today, a few examples of sanctions programs are Counter Terrorism Sanctions, Chinese Military Companies Sanctions, and Ukraine-/Russia-related Sanctions.

In some cases, sanctions cover entire regions or countries. In others, specific entities are identified by OFAC and may not relate geographically to the focus of the sanctions program. In an era of integrated financial systems, easy access to travel, and electronic communication, geography is not always the best indicator of financial ties with a sanctioned regime. For example, a Swiss company may become sanctioned under Ukraine/Russia-Related Sanctions once investigations reveal that it is almost wholly owned by a sanctioned Russian company. Companies like this often attempt to conceal their criminal ties in order to retain access to the global economy, which makes it difficult for legitimate businesses to keep track of who they can transact with.

On top of all this, the sanctions are constantly changing, with new sanctioned individuals and entities added to the OFAC SDN list daily. As the Russo-Ukrainian War continues, sanctions adjust as pieces of land oscillate between captured and liberated. The OFAC compliance efforts of every company must effectively conform to the complicated web of US sanctions regulations.

In an era of integrated financial systems, easy access to travel, and electronic communication, geography is not always the best indicator of financial ties with a sanctioned regime.

What do non-compliance penalties look like?


Violations of different sanctions regimes result in different fines, ranging from tens of thousands to millions of dollars. In 2020, a penalty of \$90,000 could be expected for a violation of the Trading with the Enemy Act. On the other hand, breaking the Foreign Narcotics Kingpin Designation Act would result in fines of \$1,500,000 for each violation. In the middle of those was the International Emergency Economic Powers Acts, violations of which had fines of about \$308,000 (source: Association of Certified Financial Crime Specialists). According to Dow Jones, UniCredit Bank, ZTE Corporation, Standard Chartered, Crédit Agricole, Société Générale, and BNP Paribas are a few companies that have had to pay huge penalties, many of which broke a billion dollars.

However, these penalty amounts are not final. The final settlement takes into account many different factors, including whether or not the violations were voluntarily or involuntarily disclosed (self-reported or hidden from OFAC), whether there have been other infractions in the past five years, and the severity of the violations (often classified as egregious or non-egregious). Ultimately, the company's attempts to avoid violations, and the actions they take once the violations are detected come into play when deciding the final penalty. Later in this paper, a few case studies on violations and their outcomes will be explored.

What constitutes a violation?

For each type of sanction, a different action may constitute a violation and result in a civil penalty. It may be difficult to keep track of what is and what is not permitted, but the OFAC official website can provide guidance as necessary. However, many companies do not engage in willing conspiracies like the British American Tobacco p.l.c., and still find themselves in violation due to oversight, rogue employees, or simple human error.

Even companies which are large and established enough to devote special attention to sanctions compliance are not always successful. As in the case of American Express National Bank in July of 2022, human error led to a sanctions violation which cost the company \$430,500. Evidently, it can be difficult to avoid the roadblocks of US sanctions, and OFAC is not shy to impose punishments for violations of its statutes. Therefore, it is important that companies of all sizes take this into strong consideration, and do their best to demonstrate their commitment to respecting the regulations.



Even large, well-established companies that devote special attention to sanctions are not always successful at ensuring compliance.

Timeline

The following is a timeline of OFAC sanctions enforcement actions from January 1, 2023 to July 1, 2023. In the graphic, Entity refers to the company which violated the sanctions, Violation refers to the sanctions program which was violated, and Fine is the penalty the company is required to pay. Disclosure is either Voluntary or Involuntary, depending on whether or not the company voluntarily self-reported the violation. Scale is a rating of either Egregious or Non-Egregious, indicating the severity of the violations according to OFAC: Egregious is very severe, and Non-Egregious is less severe.

 **Entity:** Godfrey Phillips India, Ltd.

 **Violation:** North Korea

 **Fine:** \$332,500

 **Disclosure:** Involuntary

 **Scale:** Non-Egregious

 **Entity:** Wells Fargo Bank

 **Violation:** Iran, Syria, and Sudan

 **Fine:** \$30,000,000

 **Disclosure:** Voluntary

 **Scale:** Egregious

● MARCH 01, 2023 →

● MARCH 30, 2023 →

 **Entity:** Uphold HQ Inc.

 **Violation:** Iran, Cuba, and Venezuela

 **Fine:** \$72,230

 **Disclosure:** Voluntary

 **Scale:** Non-Egregious

 **Entity:** Godfrey Phillips India, Ltd.

 **Violation:** North Korea

 **Fine:** \$332,500

 **Disclosure:** Involuntary

 **Scale:** Non-Egregious

● MARCH 31, 2023 →

● APRIL 6, 2023 →

Entity: British American Tobacco p.l.c.

Violation: WMD Proliferation and North Korea

Fine: \$508,612,492

Disclosure: Involuntary

Scale: Egregious

Entity: Poloniex, LLC

Violation: Crimea, Cuba, Iran, Sudan, and Syria

Fine: \$7,591,630

Disclosure: Involuntary

Scale: Egregious

• APRIL 25, 2023 →

• MAY 1, 2023 →

Entity: Murad, LLC

Violation: Iran

Fine: \$3,334,286

Disclosure: Voluntary

Scale: Egregious

Entity: Swedbank Latvia

Violation: Crimea

Fine: \$3,430,900

Disclosure: Involuntary

Scale: Non-Egregious

• MAY 17, 2023 →

• JUNE 20, 2023 →



Case Studies

Three enforcement actions stand out within the OFAC violations of 2023. Firstly, British American Tobacco's settlement reached over half a billion dollars, the highest fine in over a year. Microsoft reached a settlement for just under three million dollars for over a thousand violations. Finally, Wells Fargo Bank had the second highest fine in over a year, coming in at thirty million dollars exactly, a violation that brings attention to common difficulties with sanctions compliance in the finance industry. This section explores the three enforcement actions in detail, starting with the violations themselves and then considering the factors that led to OFAC's penalty decision.



April 25

British American Tobacco Inc Breaks the Record for OFAC's Highest Fine After North Korean Conspiracy is Revealed

British American Tobacco p.l.c., or BAT, is a company which manufactures tobacco and cigarettes and is headquartered in London. On April 25, OFAC released a statement on the company's violations of OFAC sanctions, and revealed that a settlement had been reached. The fine imposed on BAT involved two types of sanctions violations: Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR) and the North Korea Sanctions Regulations (NKSR). The eventual settlement was \$508,612,492, the highest fee in all of 2022 and 2023. The fine reflects both the severity of the violations (labeled as Egregious) as well as the fact that it was not self-disclosed voluntarily.

In 2001, a subsidiary of British American Tobacco in Singapore (BATM) created a joint venture alongside a North Korean company to manufacture and sell BAT cigarettes in North Korea. In 2007, due to concerns about the country's reputation, BAT executives decided to 'sell' (for one euro) the entirety of its share in the joint venture to a Singaporean company. BAT effectively retained control the entire time, and this conspiracy continued for years. Between 2009 and 2016, the North Korean company in the joint venture sent money back to BAT through a complicated process of Chinese

banks, the Singaporean company, and BATM (ending in a US bank's foreign branch). During the process, over two hundred USD payments were made between the North Korean Company and Singaporean company, which eventually brought money back to the American parent. Various communications from within the company demonstrated that the executives were aware of the restrictions on transactions with North Korea, and even attempted to hide their activities from the banks they used. Due to increasing sanctions, the last transaction was completed in 2016 and the joint venture was terminated in May of 2017. In 2016 and 2017, cigarettes were sold to the North Korean embassy in Singapore by BATM and the Singaporean company, resulting in 15 more transactions that violated sanctions (NKSR).

For its violation of WMDPSR, OFAC has fined BAT for \$503,263,807, and for its violations of NKSR, it must pay \$5,348,685. The statutory maximum was chosen because of BAT's willful conspiracy, efforts at concealment, and its positive effect on the North Korean cigarette manufacturing market, which has earned the DPRK government over \$1 billion per year.



April 6

Microsoft Settlement Articulates the Value of Monitoring Subsidiaries, Resellers and End Users.

On April 6, Microsoft reached a settlement with OFAC regarding 1,339 violations of sanctions and export controls. Microsoft will have to pay \$2,980,265.86 as penalty for allowing their services to be sold to end users in sanctioned locations, including Iran, Cuba, Syria, Russia, and Russian-occupied Crimea. They have also reached a separate settlement with the Bureau of Industry and Security, another regulatory regime, to which Microsoft will have to pay over \$600,000. This situation highlights the responsibility of companies to control and monitor their foreign subsidiaries, distributors, and resellers, who may knowingly or unknowingly bring company operations into conflict with strict American sanction laws.

The 1,339 violations occurred between July 2012 and April 2019, when Microsoft sold, activated, and provided services related to software licenses to sanctioned entities. Through incentive programs and volume licensing sales, Microsoft

used third party resellers to provide access to new customers, many of whom did not provide complete or accurate information regarding their identity. These end customers would then use US-based Microsoft servers, managed by American employees. Microsoft Russia also appeared to have deliberately attempted to hide the identity of end users as well. Compliance screenings were not conducted in an efficient manner, and often missed SDN individuals and entities due to algorithmic failures in correctly identifying customers. Ultimately, multiple long-term business arrangements with SDNs occurred within the time frame of the violations.

Because Microsoft self-reported these violations once they were discovered, and OFAC did not classify them as egregious, the fine was lowered to \$2.98 million from the base civil penalty of over \$5 million. The maximum they could have been asked to pay in this situation was \$404 million.

The Consequences of Inaction: Wells Fargo Bank Continues the Trend of Financial Sector Violations Despite Early Warnings

On March 30, OFAC released a statement that Wells Fargo had been fined \$30,000,000 for 124 sanctions violations relating to Iran, Syria, and Sudan. Between the years of 2008 and 2015, Wells Fargo and its predecessor, Wachovia Bank, provided software to a European bank which was used for trade finance transactions with jurisdictions and persons who had been sanctioned by the US. It was clear at the time that Wachovia's management should have been aware that the European bank would be using the software to transact with sanctioned entities, but a mid-level manager still authorized development and customization of a trade insourcing software for the bank's use.

After Wells Fargo acquired Wachovia, internal concerns were raised regarding the software provided to the European bank, but these alerts were ignored. According to OFAC, Wells Fargo "failed to exercise a minimal degree of caution or care in failing to identify and prevent such transactions," as seven years passed with the bank continuing to use the software platform without warning or forced termination from Wells Fargo. Wells Fargo

should have known when acquiring Wachovia that the company had a "reckless disregard" for US sanctions programs, as evidenced by its development of the software in the first place. After seven years of inaction, despite multiple warnings from senior-management levels, Wells Fargo identified the violation and suspended the program before voluntarily disclosing its apparent violations to OFAC. These violations totaled 124, and occurred between 2010 and 2015. While it was classified as Egregious by OFAC, it is also acknowledged that Wells Fargo has generally demonstrated compliance with US sanctions efforts, and therefore the violations cannot be attributed to a systemic compliance breakdown.

Wells Fargo is one of 12 financial institutions to be the subject of OFAC enforcement since the beginning of 2022. In total, there have been 22 OFAC enforcement actions reported in this time frame, which means over half of OFAC violations have been committed in the finance industry. Four of the finance companies facing penalties are cryptocurrency exchanges.

OFAC Violations by the Numbers

The story of every sanctions violation is different. Some are accidental while others are the result of elaborate conspiracies; some only involve the actions of subsidiaries while others are born from neglectful oversight of acquisition projects. Despite these distinctions, a deeper understanding is gleaned from assessing their similarities. Ultimately, analysis, segmentation, and visualization of enforcement data has made it clear that important patterns do exist.

Violations by Industry

*Between January 1, 2022 and July 1, 2023, fourteen out of twenty-four enforcement actions were made against companies in the financial industry. **Four of those were cryptocurrency exchanges.***

11

Finance



7

Other



4

Crypto



2

Tobacco



2

Metals and Mining



Penalty Distribution



This graph shows the distribution of fines between January 1, 2022 and July 1, 2023. During this period, twenty-two out of twenty-four OFAC actions resulted in fines.

The most common range of fines was \$100,000 to \$1 million.

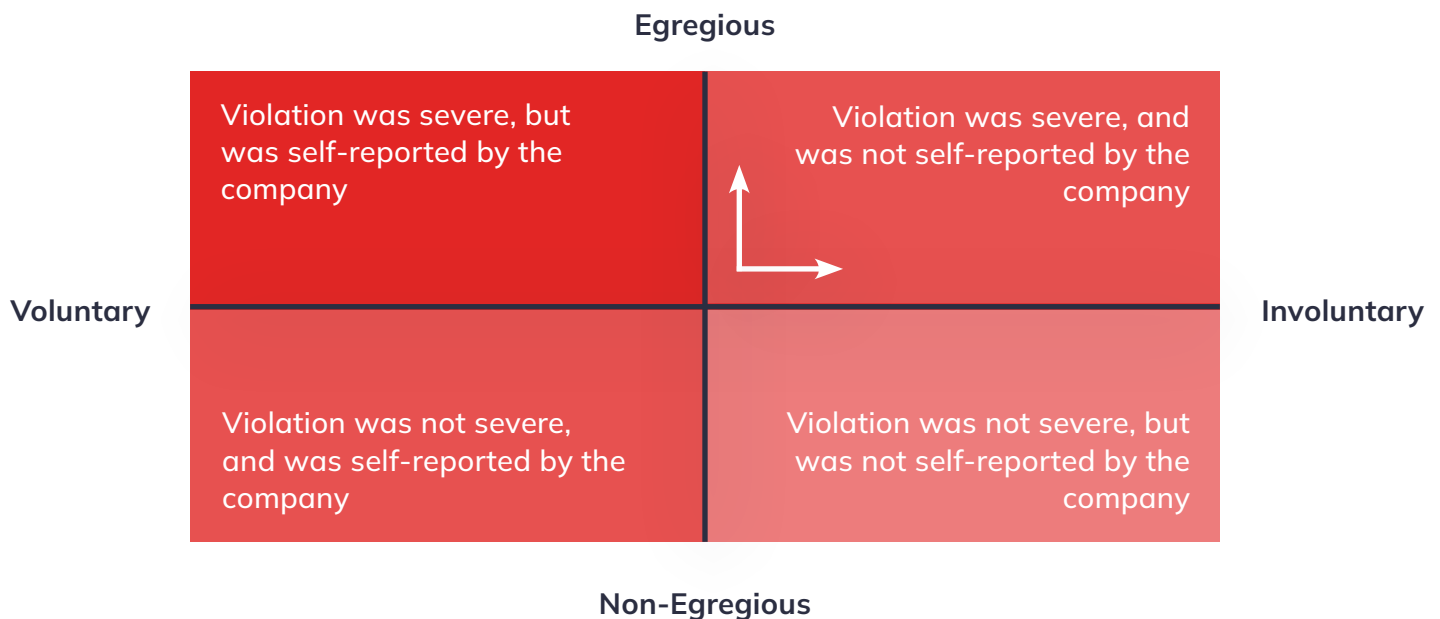
The second most common was \$1 million to \$10 million.

A single settlement was over half a billion dollars.

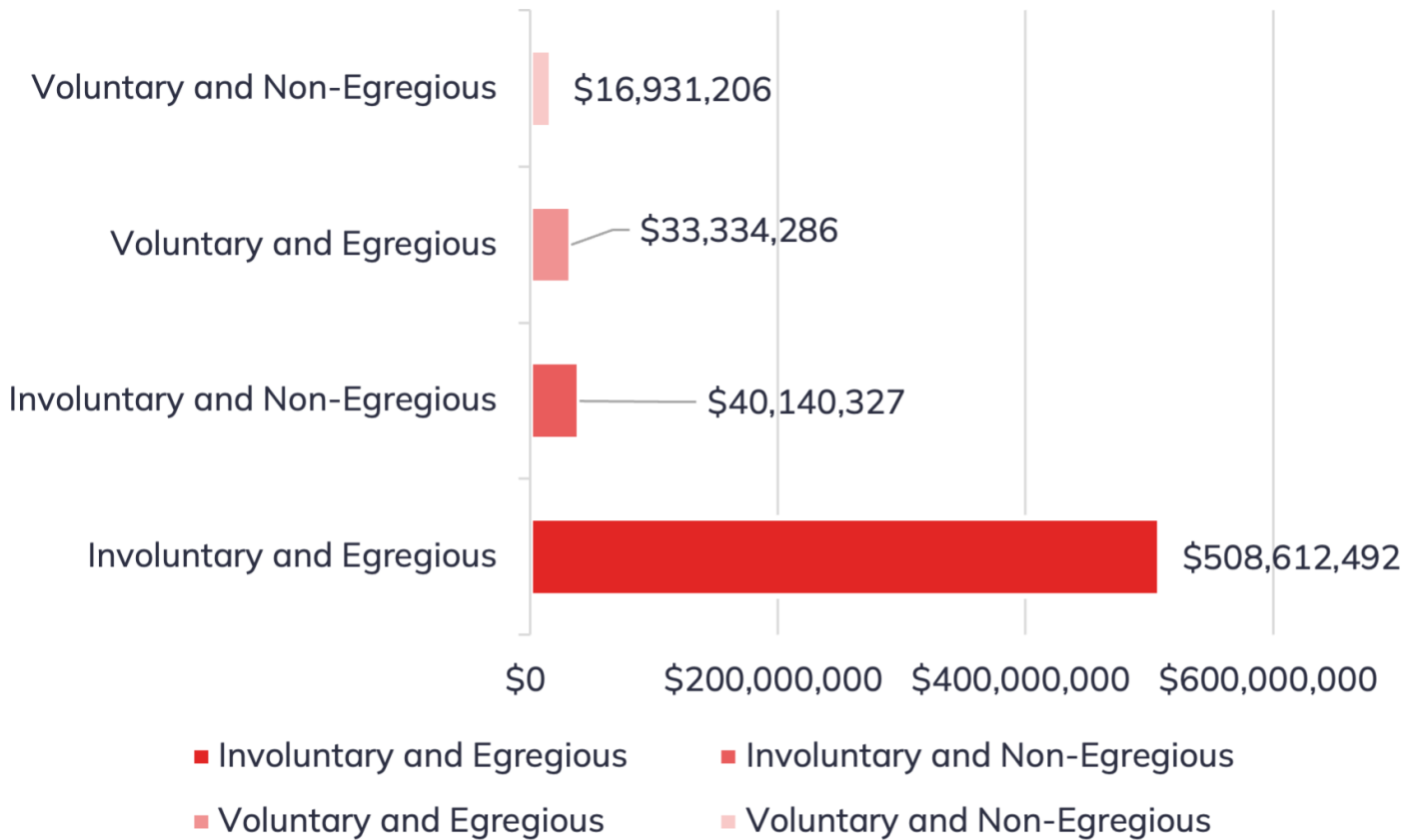
The violations are often categorized by their severity and the conditions of their disclosure. Severe violations are classified as Egregious, and less severe as Non-Egregious. If the violations were self-reported to OFAC, they are Voluntary, and if not, they are Involuntary. Generally, Egregious violations have higher fines than Non-Egregious violations, and Involuntary disclosures have higher penalties than Voluntary ones.

The highest fine between January 1, 2022 and July 1, 2023 was Egregious and Involuntary.

The following four-quadrant chart provides a visualization of the four categories: Egregious and Voluntary; Non-Egregious and Voluntary; Egregious and Involuntary; and Non-Egregious and Involuntary. Note that the penalty rises in the direction of the white arrows.



Total Fines by Quadrant



As for the total value of the fines separated into the four categories, Voluntary and Non-Egregious takes the lead over Involuntary and Non-Egregious, even though on average, Voluntary results in lower fines. This is simply because more entities chose to Voluntarily disclose their violations rather than attempt to keep them hidden.

Conclusion

Staying Compliant in a Changing Global Environment

Complying with today's volatile sanctions environment is challenging. Today, there are more designations and sanctions programs than ever before, driven by the rising pace of geopolitical and economic change. Maintaining compliance restrictions requires the ability to adapt to rapidly changing conditions on the ground and in cyberspace. Land and assets can change hands frequently, and communications may be rerouted for the sanctioned entities' use.

A rise in sanctions on countries like Russia, who are central to many global businesses, adds additional complexity. While resources such as the OFAC SDN list may provide information about sanctioned entities, the subsidiaries of these enterprises are scattered all over the world. Transacting with these subsidiaries (even those that are only partially owned) will lead to penalties, investigations, negative press, and disruption and loss of business. These subsidiaries, in places like Cyprus, Belarus, and even in your own backyard, may not be listed in official documents or found in online resources. They require investigative and digital forensic research to identify them, adding cost and complication to the perpetual cycle of becoming and remaining in compliance.

Compliance at Scale - Expertise Meets Technology

Companies can now solve this existential risk to their business using new advances in automation and technology. The ThreatSTOP platform integrates with firewalls, routers, DNS servers and other devices to block, allow, or redirect communications with unwanted entities, such as those sanctioned by OFAC on a connection-by-connection basis. If your company network cannot contact sanctioned entities, there is no way to conduct business with them. This technology protects against human error as well as unauthorized or purposefully malicious actions.

ThreatSTOP provides comprehensive sanctions coverage far more advanced and complete than any other geographic-based network enforcement solutions. The platform automatically blocks and reports machine to machine connections with sanctioned countries, entities and subsidiaries, as well as invaded and seized territories. The platform allows flexibility in enforcement policy creation, letting users choose which countries and sanctions regimes they want to block, and offering the option of actively allowing traffic on an entity-specific basis.

The ability to automate compliance efforts allows organizations to focus more time and energy on their business, while saving money and resources compared to traditional compliance approaches. By blocking and logging non-compliant communication attempts, they can prove, with verifiable data, that they're committed to meeting compliance requirements, and can trace the internal and external sources of policy violations for remediation.

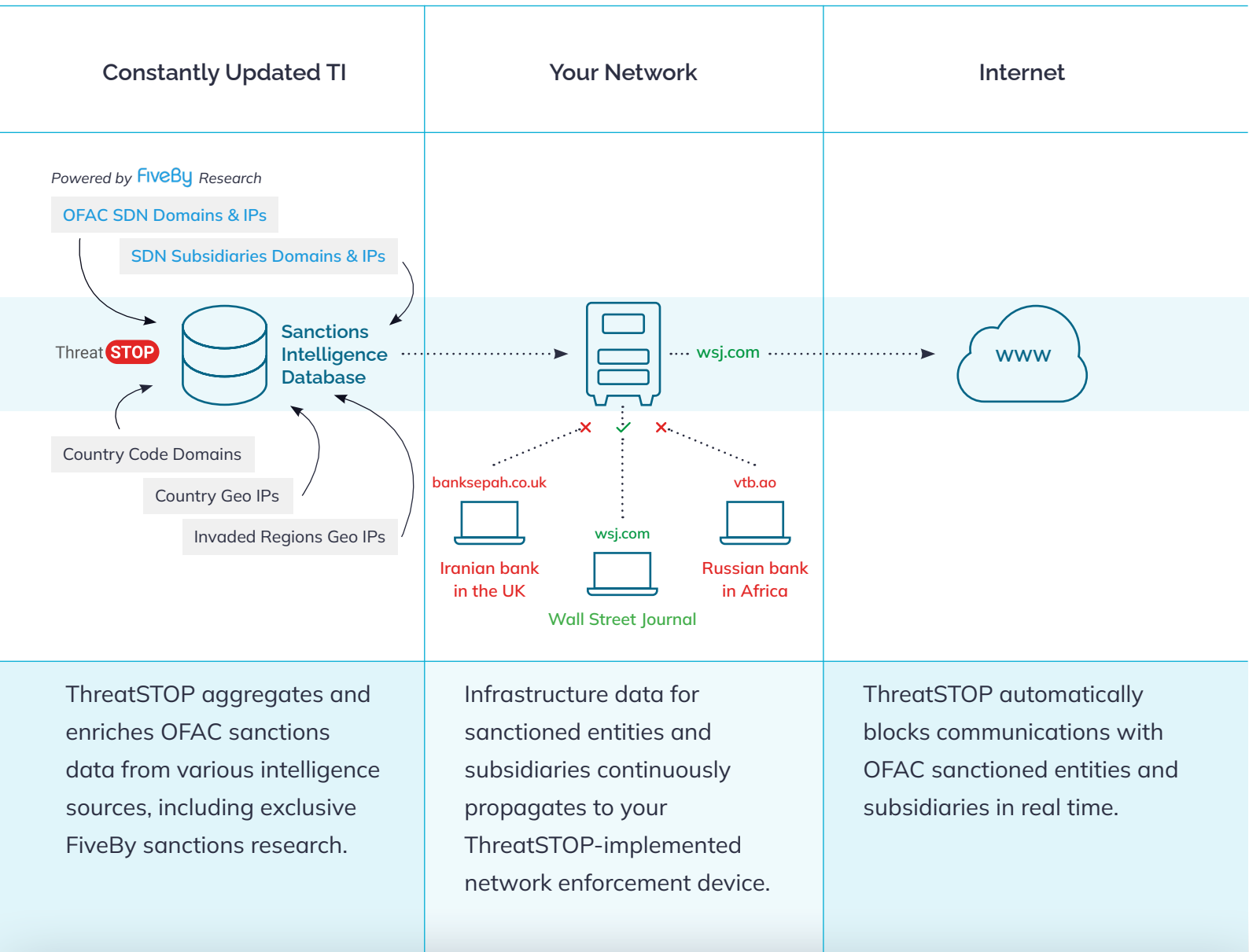
Automated Compliance with ThreatSTOP

ThreatSTOP's One-Click Sanctions Compliance is a highly effective compliance solution that proactively prevents transactions that could violate sanctions and export control restrictions by blocking internet communications with OFAC-sanctioned countries and entities, including their international subsidiaries. This not only protects businesses from potential legal consequences, but also promotes a safer and more secure global business environment.

This innovative compliance technique combines machine and human intelligence to help global businesses manage risk by preventing internet-based interactions with sanctioned entities, thus making it nearly impossible to engage in business with them. The One-Click Compliance platform offers customizable, compliance-oriented network enforcement policies that are easy to implement, with no new hardware or software.

Key Benefits:

- Automatically block sanctioned individuals, entities and subsidiaries
- Proactively prevent compliance violations instead of reacting to them
- Show stakeholders and regulators proof of successful compliance efforts
- Identify unintentional violations for quick follow-up action
- Keep focus on core business instead of compliance concerns



Conclusion

OFAC's sanctions regime is complicated, and ensuring compliance is difficult and expensive. However, companies cannot afford to ignore the issue due to OFAC's strict enforcement and costly penalties.

If you would like to continue the discussion on compliance automation, feel free to email sales@threatstop.com.