Treliant®
March 2024

INDUSTRY INSIGHTS

Steering Through 2024 Sanctions Compliance After OFAC's $1.5 Billion Wake-Up Call

By Darcy Allen, Justin Duquella, Richard Lee, and Allan Llarena

"Any institution, wherever located, that wants to reap the benefits of the U.S. financial system must also play by the rules that keep us all safe from terrorists, foreign adversaries, and crime—or face the consequences." With this statement, U.S. Treasury Secretary Janet Yellen recently reasserted her agency's heightened scrutiny of the non-traditional financial industry and its continued focus on traditional financial institutions. Now more than ever, the importance of understanding and navigating the complexity of sanctions compliance cannot be overstated.

2023 was a record year for the Treasury Department's Office of Foreign Assets Control (OFAC), as the agency imposed a combined $1.5 billion in civil monetary penalties. Although the number of enforcement actions (17) was consistent with the agency's long-term average trend, two large penalties skewed the dollar amount. One was assessed against a global tobacco company at $508 million, and the other involved a record-breaking $968 million settlement with a cryptocurrency exchange. Altogether, the agency's 2023 track record underscored that sanctions requirements must be followed and material lapses will not be tolerated.

These recent events also deliver a finer point, whether a firm operates in the virtual currency space, traditional finance, or in industries such as cosmetics and manufacturing. Specifically, senior management involvement and accountability is imperative to mitigate the risks of sanctions violations, in addition to adequate investment and continuous improvement of staffing, systems, and the other essential components of effective sanctions compliance infrastructures.

What Is a Robust Sanctions Program?

Before delving into how organizations can apply lessons learned from the 2023 OFAC violations in their sanctions programs for 2024 and beyond, it is worth revisiting some of the expectations of what constitutes an adequate sanctions compliance program (SCP). Key components include:

- **Leadership:** Senior management must support sanctions compliance by delegating sufficient authority and autonomy to compliance teams to effectively implement controls that manage an organization's OFAC risk, ensuring they have the necessary resources, approving and overseeing the SCP, encouraging a culture of compliance, and understanding the importance of adhering to regulations.
- **Risk Assessments:** Routine OFAC sanctions risk assessments must evaluate an organization's exposure to OFAC sanctions risks, the results of which should be used to inform the development or enhancement of internal controls to appropriately manage such risks, and to also update the sanctions risk assessment methodology, as appropriate.

- **Controls:** A system of internal controls (i.e., clear, defined, and documented procedures and processes), in part leveraging information from risk assessments, recent audits and/or exams, and internally identified deficiencies and corrective actions, should be used to help detect, prevent, report, and document activities that violate OFAC regulations. This also includes having software and systems that are fit for purpose, calibrated, and tested.
- **Audits:** A testing/auditing function must conduct regular reviews of the compliance program to uncover and rectify any issues, thereby enhancing the program's effectiveness.
- **Training:** Employees should be provided with continuous and relevant training on their roles and duties in the SCP, tailored to an organization's risk profile and informed by, and responsive to, issues identified through the risk assessment, testing, and/or audits to address any deficiencies.

Themes Emerging from 2023 OFAC Sanctions Violations

OFAC's enforcement spotlighted several different industries in 2023, emphasizing the necessity for improved compliance infrastructures across a broad spectrum of businesses.

- The virtual currency sector bore the most significant impact through four penalties totaling nearly $977.5 million for violations involving Crimea, Iran, and Syria. This underscores the regulatory emphasis on the complexities of digital finance and the importance of calibrating and testing interdiction and screening software to ensure comprehensive compliance.
- The tobacco industry faced substantial fines of $508.9 million, highlighting the need for industry-specific compliance strategies.
- Traditional finance firms, including banks and payment services, were fined over $37.7 million, reflecting the challenges in deploying robust know your customer (KYC) systems.
- The manufacturing and cosmetics sectors were scrutinized for deficiencies in monitoring high-risk activities and due diligence, respectively, with the technology and insurance sectors also facing penalties.

Of particular note for those operating in the virtual currency space, or any other organizations that give access to users/customers to payment rails, is the importance of monitoring internet protocol (IP) addresses for those accessing these platforms and networks. Geofencing and virtual private network (VPN) detection tools should also be implemented as a preventive measure to mitigate the risks of actors accessing platforms from sanctioned jurisdictions. Ensuring the effectiveness of these programs requires substantial investment in compliance infrastructure, sufficient and skilled staffing, continuous training, and strict adherence to compliance protocols to avert legal and financial risks.

In addition to what one could learn from the penalties impacting the virtual currency sector, below is a summary of thematic issues observed in 2023 across various industries.

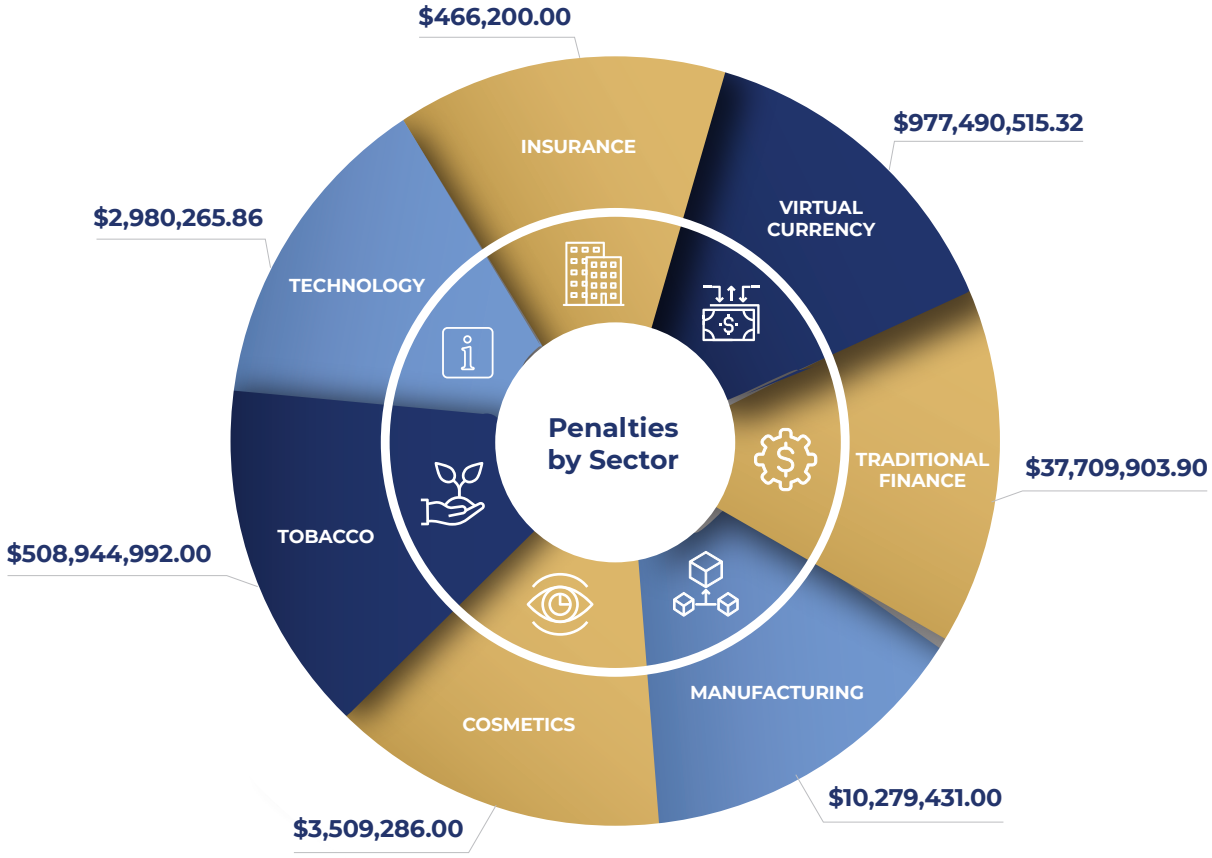

Figure 1 – Summary of Penalties by Sector

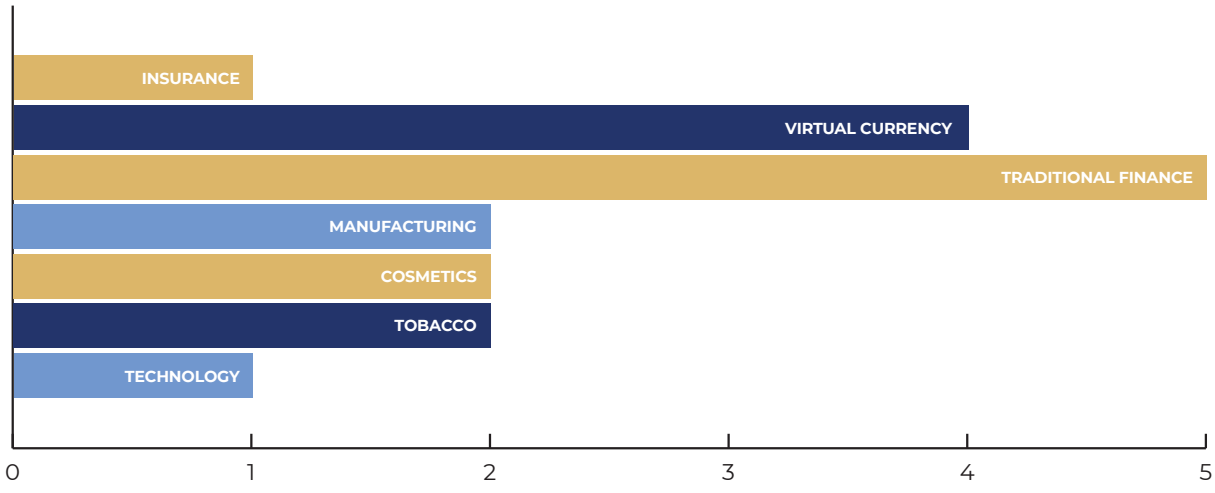

Figure 2 – Number of Penalties by Sector

- **Financial Services:** Compliance issues mainly due to poor transaction and client monitoring, outdated technology, and insufficient due diligence, leading to significant penalties for failing to act on internal warnings.
- **Tobacco:** Turning a blind eye to compliance for profit through document falsification, hiding dealings with sanctioned entities, and using intermediaries to mask true transaction beneficiaries.
- **Manufacturing:** Exports to banned entities by foreign subsidiaries due to lack of oversight and attempts by employees to bypass sanctions, indicating poor internal controls and training.
- **Cosmetics:** Illegal exports to a sanctioned country by senior executives without necessary licenses, showing the lack of an effective compliance program and oversight.
- **Technology:** Inadequate screening mechanisms that resulted in dealings with prohibited entities, highlighting ineffective compliance systems and beneficial ownership verification failures.
- **Insurance:** Failures of due diligence and screening processes to detect transactions involving sanctioned jurisdictions.

Considering Sanctions in 2024 and Beyond

The recent penalties and violations suggest rising regulatory expectations for a robust SCP. As such, they should remind senior management and those heading sanctions compliance programs that there is a need to continuously revisit, refresh, and revise SCPs. To manage sanctions risk exposures, ask yourself the following:

- Are screening and interdiction tools used by your organization sufficient, appropriately calibrated, tested, and maintained to react to ever-changing sanctions and embargoes regulations? Or is there a business case to update, enhance, or even replace these tools to enable sufficient coverage for the organization's sanctions risk profile?
- Are all relevant fields for screening covered by screening tools, including addresses, email suffixes, passports, phone numbers, nationalities, and postal codes (not just names and country fields)? Are there controls in place to ensure proper screening?
- Are tools and technologies employed to enable geofencing and detection of users that access platforms through a VPN?
- Is KYC data captured by your organization in non-Latin scripts such as Cyrillic, Chinese, or Arabic? Is your screening program robust enough to handle non-Latin scripts via translation and/or transliteration?
- For U.S. legal entities, are you also screening for beneficial owners that meet the "50% Rule"?
- Do you operate in high-risk regions within close proximity to sanctioned jurisdictions, and are there proper controls and oversight of business units in those regions from a sanctions perspective?
- Has your organization undergone recent mergers or acquisitions? If so, has sufficient pre- and post-merger due diligence been performed related to sanctions exposure, integration, training, and uplifting the SCP?
- Does your organization have adequate staff with experience and knowledge in sanctions matters, to handle outputs from screening and interdiction processes?

Conclusion

In 2023, OFAC's enforcement actions, totaling $1.5 billion in penalties, underscored the necessity for stringent sanctions compliance across all sectors. This emphasizes the importance of robust screening practices, including beneficial ownership and specific address details, and the necessity for organizations to heed risk assessments, ensure adequate staffing, and maintain a workforce knowledgeable in sanctions compliance.

As we look toward 2024, organizations must focus on these SCP pillars to navigate the complexities of international sanctions effectively. It will be critical to integrate comprehensive data analysis, from KYC to transactional details, into a dynamic sanctions compliance framework. This approach, coupled with senior management's active engagement and continuous improvement of compliance infrastructure, positions firms to adequately mitigate the risks of OFAC violations. In short, if you're part of the U.S. financial system, you can either play by the rules or pay a hefty price.

Darcy Allen
Darcy Allen has over 25 years of financial crimes compliance experience spanning government, consulting, banking, and retail. Darcy started his career with the Canadian government, working within the Canada Border Services Agency (CBSA), which included leading a national team of customs intelligence and investigations officers working as part of the Integrated Proceeds of Crime (IPOC) joint force operation with several government organizations, including the Royal Canadian Mounted Police (RCMP). In this role, he participated in the creation and implementation of the Canadian government's Proceeds of Crime (Money Laundering) and Terrorist Financing Act. This act established the Financial Transactions and Reports Analysis Centre (FINTRAC) as well as the cross-border reporting of currency, for which he was instrumental in securing funding for the currency detector dog (K-9) program. **DAllen@treliant.com**

Justin Duquella
Justin Duquella is a Senior Manager with Treliant. With over 10 years' experience in the financial services industry, Justin has held fraud and Anti-Money Laundering (AML) compliance roles in both the banking and fintech sectors. He has extensive knowledge of fraud risk assessments, remediation action plans, suspicious activity report (SAR) writing, know your customer/know your business (KYC/KYB) obligations, account investigations, Office of Foreign Assets Control (OFAC) regulations, Financial Crimes Enforcement Network (FinCEN) requirements, Bank Secrecy Act (BSA), and Patriot Act rules including 314(a)(b) information sharing. **JDuquella@treliant.com**

Richard Lee
Richard Lee is an Analyst at Treliant. He is an adept and experienced Bank Secrecy Act / Anti-Money Laundering (BSA/AML) specialist with a passion for preventing financial crime. At Treliant, Richard brings his expertise in transaction monitoring and client due diligence to bear in helping financial institutions comply with regulatory requirements and prevent financial crime. **RLee@treliant.com**

Allan Llarena
Allan Llarena, Senior Director with Treliant, has over 15 years of experience helping various sized financial institutions in the U.S., Canada, and Europe to identify, investigate, and mitigate financial crime risk. With a heavy focus on complex international money laundering and fraud investigations, know your customer (KYC), and enhanced due diligence (EDD), as well as Anti-Money Laundering (AML) risk assessments, Allan's years of experience were gained in-house from working in AML compliance departments of large global financial institutions as well as from being a client-centric practitioner in the professional services industry. **ALlarena@treliant.com**

The Treliant Advantage

In navigating the complex landscape of sanctions compliance, organizations across industries, from traditional and non-traditional banking institutions, as well as technology, and manufacturing, all face multifaceted challenges, including inadequate due diligence, ineffective screening mechanisms, management's evasion of controls, and a lack of robust compliance programs. These challenges are compounded by beneficial ownership issues, where the true beneficiaries of transactions are obscured, leading to unintentional engagements with prohibited entities and regions.

Treliant addresses these critical issues head-on, offering specialized compliance solutions that go beyond mere regulatory adherence. With Treliant's expertise, organizations can transform their approach to sanctions compliance, ensuring efficient and effective due diligence, screening, and identification of beneficial ownership, thereby mitigating risks and safeguarding against the intentional or inadvertent circumvention of sanctions regulations. Leveraging our comprehensive suite of services ensures compliance integrity across all operational facets.

In an era where the stakes of non-compliance are higher than ever, partnering with Treliant empowers your business to navigate the complexities of global sanctions with confidence.

DELIVERY MODELS