Taking a Bite Out of Sanctions Crime: KleptoCapture Enforcement and the New FCPA

FEATURED EXPERTS

David Tannenbaum, Director, Blackstone Compliance Services
Cynthia Hetherington, Founder & President, **Hetherington** Group
Eric Young, Senior Managing Director, Guidepost Solutions

MODERATOR

Laura Klein, Director of Business Intelligence, RANE

Moderator **Laura Klein** began the webinar by asking the panelists to describe their backgrounds and experiences with sanctions enforcement.

- **Eric Young** observed an evolution of greater global coordination among Western nations that links effective compliance with national security.
- **Cynthia Hetherington** noted that staying and remaining one step ahead is crucial to mitigate problems, such as knowing your customer. She has observed that while there was a greater amount of deregulation of compliance under the Trump administration, companies actually increased and intensified training.
- **David Tannenbaum** noted that the current sanctions program against Russia has shown more of a sense of urgency and a national priority, which had not generally been there in past sanctions programs. The seriousness of the situation also meant that there are a series of non-financial sanctions such as port and airspace bans or prohibitions on incorporation services which had been mostly absent from past sanctions programs.
- **Young** added knowing who your customer is and their vendors helps connect the dots within the supply chain to better understand who and which entities are regulated and / or at risk of sanctions evasion or violations.

Klein then asked the panel to discuss compliance around the Metaverse.

- **Hetherington** spoke about a project called Operation Vax, where, in coordination with pharmaceuticals, security experts, open-source intelligence gatherers, and boots-on-the-ground monitoring helped ensure the safe and secure transportation, storage, and distribution of the Pfizer, Moderna, AstraZeneca, and Johnson & Johnson vaccines. She noticed movement on the dark web and with concerns of money laundering and trafficking that are moved through these platforms, she recognizes a need to understand the new Metaverse and the compliance nightmare it will create due to lack of controls.
- **Young** spoke about the Metaverse being used by criminals in virtual games. He finds a major concern is monitoring and surveilling activity and electronic communications through social media. The Metaverse adds an element that puts this sector further behind, “unless firms, regulated and now unregulated,

have sanctions compliance programs, enterprise compliance programs, which the DOJ and other enforcement agencies have long expected."

Next, **Klein** asked the panel what they see as being the most important part of Know-Your-Client (KYC) programs.

- The first step is untangling the regulators' rules around which KYC rules apply, as some regulators such as FinCEN allow firms to stop their KYC at the first level of the customer while OFAC expects the KYC to pierce the corporate veils all the way to ensure that we know whether the UBO is sanctioned or not, noted **Young**. "That's because accounts are not static, and ownership's not static," so it's a task of understanding the movement of assets and accounts and being able to freeze them and report them not just for management purposes but to protect our national security as well as protect the firm from prosecution.
- **Hetherington** experienced the program at her company because it allowed her to look at the company from a holistic view and to do a gap analysis of their own situation. She empathized with identifying these gaps as pertinent to doing business, as she has seen too many companies where not only do they *not* have a robust security system in place, but compliance is secondary.
- KYC is going to be the most important control for sanctions because sanctions are predicated on ownership, said **Tannenbaum**. OFAC, the E.U., and other authorities consider a company or asset to be subject to sanctions if it is owned, 50% or more in the aggregate, by sanction persons. Many sanctions targets have evaded sanctions through reliance on shell or front companies.
- **Tannenbaum** noted that one of the biggest struggles in the KYC process comes down to the quality of data stored on the customers (which can inhibit identifying sanctions targets in the future) and the ability to verify ownership – particularly of complex ownership structures.
- **Young** said the culture of the organization that has to comply is critical, as you are only as good as your weakest link. For example, firms invest in business products and technology, but cut back or hold back on investing in regulatory technology to effectively implement artificial intelligence to track – and predict – financial crimes including sanctions evasion or illegal payments attempts. In North Am**eric**a, over 40 billion dollars is spent on AML and sanctions compliance added **Tannenbaum**. While bad guys have changed tactics over the past decade, regulators and how regulations are written have not changed in tactics, which has "encouraged a lot of inefficient compliance controls designed to appease strict liability as opposed to conduct an efficient financial intelligence investigation," suggested **Tannenbaum**.

In anticipation of the webinar, a poll conducted by RANE asked what people saw as the greatest challenge to the KleptoCapture task force. Half of the respondents indicated that they thought it would be corporations from countries historically known as money laundering jurisdictions. **Klein** asked the panel what they thought of the response and if there were other challenges on the horizon for the task force.

- KleptoCapture has teeth, said **Hetherington**, so it goes after oligarchs and their families and finds the weakest link, as it can help incite an emotional response in wartimes, which is tactical in terms of strategy. Currently, the media has run circles around the task force due to the leaks such as the Panama Papers, FinCEN leaks and Paradise Papers. The education to support public relations is not there yet.
- **Young** noted there are also many non-Western countries that are not participating in sanctions. The public-private partnerships under the AML Act of 2020 are critical including the required US government registration of the ultimate beneficial owners with the goal of enabling industries and suppliers canto tap meaningfully.
- **Tannenbaum** noted that The Department of Justice (DOJ) has been implementing sanctions for a long time, and a portion of the enforcement actions that come out of OFAC is from the DOJ. While asset forfeiture has been in place for about a decade, under KleptoCapture, seizures of assets have been easy due to locations and the European allies being more aggressive in assisting the U.S. with the cases. Those in Turkey and the UAE are going to be harder as those countries are not as cooperative and the United States has not had an MLAT with these jurisdictions before.

Klein then asked about certain national security issues, such as those around food supply and the need for identifying people behind keyboards.

- Compliance is not just about fairness but also security, suggested **Hetherington**. CFIUS is specifically about national security, and much of her experience is monitoring nation-states and watching how they steal the intellectual property of her customers, through counterfeit products, from jewelry to pharmaceuticals. Understanding what these nation-states are doing requires getting inside your networks, infrastructure, and financial service systems, and at each stage, the United States falls behind in protecting assets, observed **Hetherington**. Having a good compliance system instead of just paying off fines is key to posturing a system that protects its assets, she concluded.
- We are moving into a unipolar world, added **Tannenbaum**, where multiple great powers are competing against each other. OFAC needs to be able to collaborate better with other parts of the government and private industry.
- For example, OFAC has involved itself in cyber security issues – particularly ransomware attacks made by a sanctioned threat actor – but does not seem to have been able to work well with other government agencies such as CISA or the private sector to actually provide actionable guidance.
- It's not all doom and gloom. Russia has involved a more proactive and collaborative approach from governments towards sanctions, **Tannenbaum** predicted.
- **Young** expressed concern that companies will cut back on spending due to the world heading towards a recession and thus impeding the process. With these concerns, plus inflation, and supply chain risks, companies need to commit to what needs to be done going forward, stressed **Young**.

Klein concluded the discussion by asking the panel if there were anything they would touch back on.

- "While we do call this the "new FCPA", we still cannot forget the old FCPA, because none of these risks are mutually exclusive. Bribery and corruption help grease the wheels of sanctions evasion, and therefore impact our national security," concluded **Young**.
- At the base level, cities and states need to stay within a standardization of compliance for protecting their own assets, said **Hetherington**. "Companies like RANE, and experts like **Tannenbaum** and **Young**, can help with that. It takes a community. It takes a village. And we would be much safer and smarter," to not continuously lean on the DOJ to fix problems, **Hetherington** concluded.
- **Tannenbaum** highlighted an advisory that was published through RANE on a blueprint for where to take your compliance program to make Russia's sanctions sustainable.

ABOUT THE EXPERTS

Cynthia Hetherington, Founder & President, **Hetherington** Group

Cynthia Hetherington, MLS, MSM, CFE, CII is the founder and president of Hetherington Group, a consulting, publishing, and training firm that leads in due diligence, corporate intelligence, and cyber investigations by keeping pace with the latest security threats and assessments. She has authored three books on how to conduct investigations and annually trains over 7,200 investigators, security professionals, attorneys, accountants, auditors, military intelligence professionals, and federal, state, and local agencies on best practices. Ms. Hetherington is a Subject Matter Expert and OSINT Instructor at the National Security Agency's Center of Academic Excellence in Cyber Operations (CAE-CO) and Cyber Defense (CAE-CD); an Adjunct Instructor at the University of Arizona's College of Applied Science & Technology (CAST); and an OSINT Instructor at the Department of Defense's United States Special Operations Command (USSOCOM).

For more than 25 years, Ms. Hetherington has led national and international investigations in corporate due diligence and fraud, personal asset recovery, and background checks. With a specialization in the financial, pharmaceutical, and telecommunications industries, her investigations have recovered millions of dollars in high profile corruption cases, assisting on the investigations of the top two Ponzi cases in United States history.

David Tannenbaum, Director, Blackstone Compliance Services

David Tannenbaum started his career in sanctions compliance at the Office of Foreign Assets Control's (OFAC) compliance branch where he led a team of analysts examining all rejected and blocked assets and created better processes to identify violations, emerging threats and increased information sharing between the various divisions of OFAC.

Mr. Tannenbaum created Blackstone Compliance Services, a company specializing in sanctions and AML compliance after joining the private sector in 2013. As the director of Blackstone, Tannenbaum has led sanctions testing for three major monitorships on behalf of the US Department

of Justice, Federal Reserve Board and New York Department of Financial Services. This testing has included a review of policies and procedures, compliance IT infrastructure and audits of high risk branches and affiliates.

Eric Young, Senior Managing Director, Guidepost Solutions

Eric T. Young advises highly regulated organizations on reengineering compliance, ethics, and regulatory technology programs to enable reputable and sustainable business growth. He has deep regulatory experience having spent close to 40 years in chief compliance officer roles at some of the world's largest institutions, including five global banks. Mr. Young focuses on building and sustaining enterprise compliance programs aligned with the U.S. Department of Justice Sentencing Guidelines, the rules and regulations enforced by the Federal Reserve Board, US Treasury including Comptroller of the Currency, Consumer Financial Protection Bureau, New York State Department of Financial Services, and UK Financial Conduct Authority, as well as the Bank Secrecy Act, Foreign Corrupt Practices Act, and Basel Standards.

Laura Klein, Director of Business Intelligence, RANE

Laura Klein joined RANE as the Director of Business Intelligence in December 2021 with 15 years of experience in the due diligence industry. Prior to RANE, Ms. Klein served as a Senior Director at Kroll with the company's Forensic Intelligence & Investigations practice where she managed teams assisting clients in making risk management decisions by conducting corporate intelligence investigations, locating and interviewing witnesses, asset searches, threat assessments, and fraud investigations. During the first year of the pandemic, Ms. Klein also worked to develop and publish Kroll's COVID-19 Heat Map forecasting the impacts of the pandemic across multiple geographies and sectors. Before working for Kroll, Ms. Klein served as a Managing Consultant for Navigant (now Guidehouse) with the company's Global Investigations & Compliance practice. While with the company, she specialized in fraud investigations, Foreign Corrupt Practices Act due diligence, and Enhanced Due Diligence engagements. Ms. Klein also assisted in the creation, implementation, and management of anti-corruption third party due diligence programs for Global 500 companies. She began her career at a small private investigations firm, Corporate Resolutions, where she served as hiring manager and focused on litigation support investigations. Ms. Klein received both her Bachelor of Arts and Master of Science degrees from the University of Pennsylvania and has been a Certified Fraud Examiner since 2009.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is a global risk intelligence company that provides risk and security professionals with access to critical insights, analysis, and support, enabling them to more effectively anticipate, monitor, and respond to emerging risks and threats. RANE clients benefit from improved situational awareness, more efficient access to relevant intelligence and expertise, and better risk management outcomes. Join the millions who are tapping into the collective wisdom of the world's largest community of risk and business professionals. For more information about RANE, visit www.ranenetwork.com.