WHITE PAPER

How financial institutions can address sanctions compliance in an evolving landscape

KAUFMAN ROSSIN

Learn more at kaufmanrossin.com

Many financial institutions invest a great deal of time, effort, and money in sanctions compliance. Yet, detecting and preventing sanctions evasion remains a challenge.

As the U.S. government continues to sharpen its focus on illicit activities and sanctions evaders, financial institutions are on the front line in this fight, focusing on identifying and blocking accounts and other property, as well as rejecting transactions and reporting transactions. This increasing government and regulatory focus make it more critical than ever for financial institutions to have a robust sanctions compliance program.

A robust program combines strong policies, procedures, and controls with well-trained people, automated screening tools (ASTs), and other types of automation. It should also include a comprehensive risk assessment, appropriate transaction monitoring and screening tools, as well as processes aligned with an organization's risk profile.

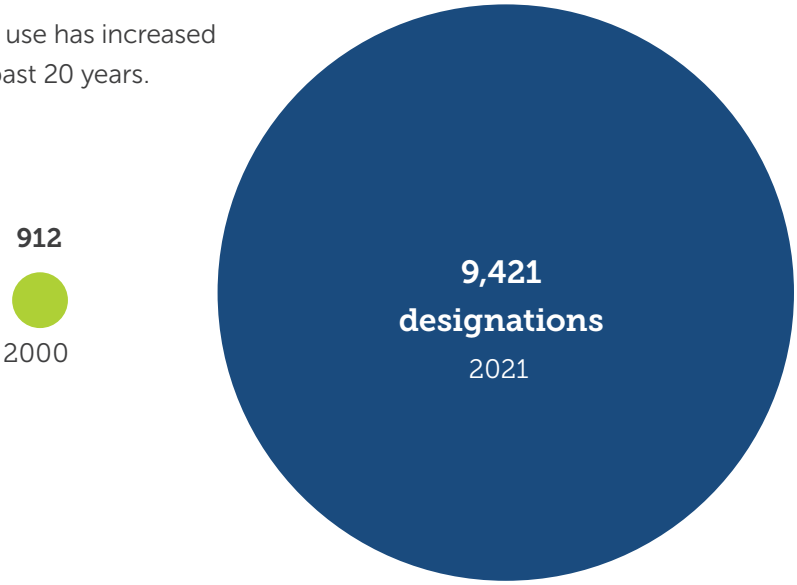
The attacks of September 11, 2001, represented a paradigm shift in U.S. foreign policy, with economic sanctions becoming a primary tool in the United States efforts to combat and prevent national security threats. Sanctions are a particularly effective tool because of the strength and global presence of the U.S. financial system, allowing the United States to impose direct and material losses on adversaries and thereby disrupting maligned behavior.

This responsibility is expanding, as sanctions regimes and actions have steadily increased in the past 20 years. Likewise, the nature of the global financial infrastructure has also increased in complexity with the introduction of digital currencies, alternative payment platforms, and new ways to conceal cross-border transactions. Bad actors can use these technologies to store and transfer funds outside of the standard dollar-based banking system, and therefore financial institutions must also implement robust sanctions compliance programs necessary to safeguard the U.S. financial system, as well as keep up with regulatory expectations.

Sanctions use has increased over the last 20 years

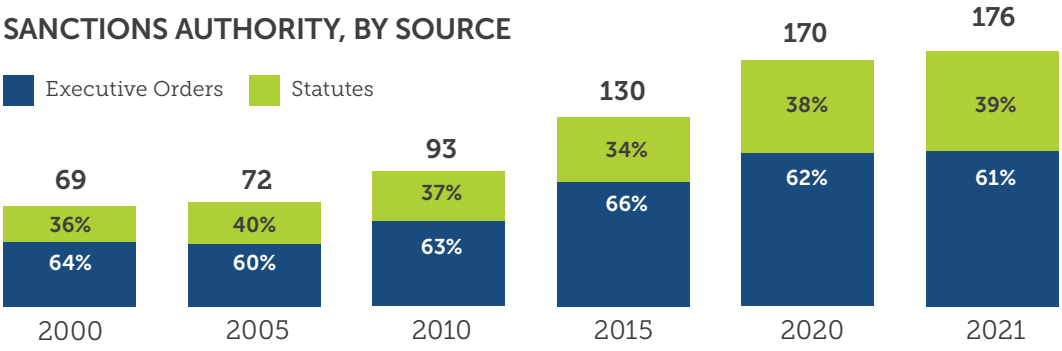
OFAC SANCTIONS DESIGNATIONS (NET)

Sanctions use has increased over the past 20 years.



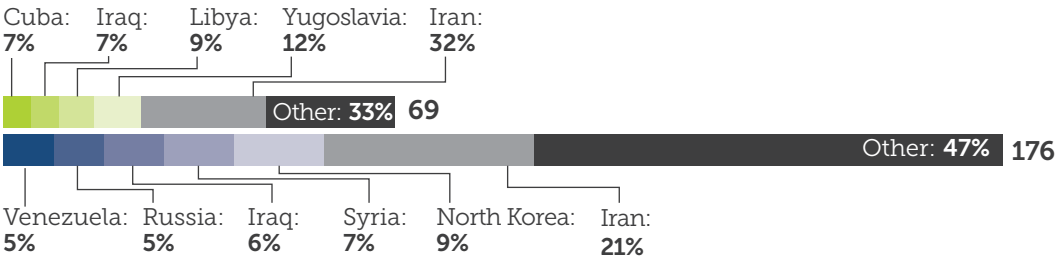
Sources of sanctions authority have been relatively constant

SANCTIONS AUTHORITY, BY SOURCE



Composition of U.S. sanctions programs shifted

NUMBER OF SANCTIONS AUTHORITIES



Source: The Treasury 2021 Sanctions Review

Today's sanctions compliance landscape

On June 16, 2021, the U.S. House of Representatives held a hearing, "Schemes and Subversions: How Bad Actors and Foreign Governments Undermine and Evade Sanctions Regimes." Several experts testified and took questions from the Committee on Financial Services' Subcommittee on National Security, International Development, and Monetary Policy. Representatives wanted to understand methods utilized by bad actors to evade sanctions; and techniques used to detect, prevent and report illicit activity. The Representatives also engaged the experts regarding legislative actions that could be employed to strengthen the U.S. sanctions regime.

Later that month, the Financial Crimes Enforcement Network (FinCEN) emphasized the importance of sanctions compliance in a document titled "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities."

Under Office of Foreign Assets Control (OFAC) rules, financial institutions must prevent and report, as appropriate, transactions involving a sanctioned entity, individual, property or service. OFAC enforces this on a "strict liability" basis, and violations may result in imposing a civil monetary penalty.

Financial institutions implement OFAC sanction compliance programs which come at significant human capital and financial costs. A June 2021 report published by LexisNexis Risk Solutions entitled, True Cost of Financial Crime Compliance Study, Global Report, indicated that the projected total cost of financial crime compliance in the United States was $35.2 billion and cited sanctions screening as a top challenge with financial crime compliance operations facing financial institutions in North America.

Significant illicit financing threats facing the U.S.

In June 2021, FinCEN, in consultation with other government agencies, regulators, law enforcement and national security agencies, issued the "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities." This document laid out the U.S. government's current AML/CFT priorities, which include:

- Corruption
- Cybercrime, including relevant cybersecurity and virtual currency considerations
- Foreign and domestic terrorist financing
- Fraud
- Transnational criminal organization activity
- Drug trafficking organization activity
- Human trafficking and human smuggling
- Proliferation financing

Additional guidance, administrative rulings, and illicit finance information (including advisories and notices) can be found on FinCEN's website at www.fincen.gov

Why is sanctions compliance such a challenge?

There are several reasons sanctions compliance remains a challenge for financial institutions, including:

- *The size and stability of the U.S. financial system, combined with the dollar's ubiquity, make U.S. financial institutions a highly desirable target for holding or moving illicit funds.*
- *The U.S. sanctions regime has more than 30 different sanctions programs. Yet, there is not a national center dedicated to detecting and degrading sanctions evaders and their networks.*
- *A large volume of foreign funds and transactions are intermediated through correspondent banks.*
- *Sanctions evasion techniques continue to evolve, and sanctioned parties use complex structures and assets.*
- *Sanctions screening depends largely on the quality and completeness of the information provided to a financial institution.*
- *Uneven anti-money laundering obligations leave certain financial services providers and intermediaries outside the Bank Secrecy Act (BSA) scope*


K R

A framework for OFAC compliance commitments

On May 2, 2019, OFAC published A Framework for OFAC Compliance Commitments, a first-of-its-kind document outlining five essential components that all well-established sanctions compliance programs should have. This publication also contains a non-exhaustive list of common root causes of sanctions violations identified by OFAC during past investigations, which is a helpful tool in recognizing areas of improvement for existing sanctions compliance programs. OFAC advocates that each program should be constructed with a risk-based approach that considers an institution's size, products and services offered, as well as customer and geographies serviced. However, all sanctions compliance programs must incorporate the five following essential components.

1. MANAGEMENT COMMITMENT

OFAC considers management commitment as one of the most important factors in evaluating a sanctions compliance program's success. This is because this support is essential in ensuring that the program receives the resources and tools necessary to carry out its mission and is fully incorporated into the organization's daily operations. Compliance personnel should particularly welcome this component as it also asks senior management to be responsible over providing adequate resources to ensure a robust sanctions compliance program. OFAC measures senior management commitment by looking at whether the institution has designated an OFAC sanctions compliance officer and evaluating the quality and experience of the personnel dedicated to running the sanctions compliance program. This personnel should possess adequate technical knowledge over OFAC's regulations, processes, and actions and how these interrelate with complex financial and commercial activity.

2. RISK ASSESSMENT

OFAC indicates that all risk assessments should consist of a holistic review of the organization from top to bottom that assesses its touchpoints to the outside world, designed to identify potential areas in which it may engage with OFAC prohibited persons, parties, countries, or regions directly or indirectly. The risk assessment should consider (i) the institution's customers, supply chain, intermediaries, and counterparties; (ii) the products and services it offers, including how and where such items fit into other financial or commercial products, services, networks, or systems; and (iii) the geographic locations of the organization, as well as its customers, supply chain, intermediaries, and counterparties.

3. INTERNAL CONTROLS

OFAC expects that a sanctions compliance program should include internal controls utilized to identify, interdict, escalate, report (as appropriate), and keep records about activity that may be prohibited by the regulations and laws administered by the agency. These controls should outline clear expectations and defined procedures and processes pertaining to OFAC compliance while minimizing those risks identified by an institution's risk assessment. While it is essential to have these controls documented easily accessible, they mean little if not properly enforced. For this reason, internal and external reviews and assessments of the program should be regularly performed to identify any gaps.

4. TESTING AND AUDITING

Periodic reviews over sanctions compliance assess the program's effectiveness and allow for the discovery of inconsistencies between what's contained in your policies and procedures, and what's practiced in the day-to-day operations of your institution. Therefore, you must ensure that your program is subject to comprehensive, independent, and objective testing that ensures you learn how the sanctions compliance program is performing as well as how it could be updated, enhanced or recalibrated to account for changing risks.

5. TRAINING

OFAC expects that training over the sanctions compliance program should be provided to all appropriate employees on at least a yearly basis. This training must include job-specific knowledge based on need, and it must also communicate the sanctions compliance responsibilities for each employee. Finally, institutions should hold employees accountable for sanctions training through assessments.

Common methods used to evade sanctions

Bad actors looking to evade sanctions continue to use traditional fraud schemes and increasingly use the internet to facilitate fraud.

INTERNATIONAL TRADE

Trade finance transactions (including global correspondent banking, with its central role in processing dollar-based transactions and facilitating cross-border trade) are an area of vulnerability. Problematic trade transactions generally involve a complex web of several parties across the globe. These transactions facilitate the movement of money by sanctioned parties who often provide inconsistent, conflicting, or false documents related to the parties involved, the goods being shipped, the jurisdictions involved, and the vessel and shipping routes used. Weak or inconsistent controls or supervision in some foreign jurisdictions open the system to exploitation. U.S. banks that receive funds or instructions for a funds transfer from a foreign correspondent may receive limited details about the payment's originator. The U.S. bank is unlikely to have an account relationship with the originator, who may not even be a direct client of the respondent.

COMPLEX STRUCTURES AND ASSETS

Complex structures and assets, including those that combine shell companies and companies with legitimate business purposes, allow sanctioned actors to obscure their ownership of transacting entities.

The use of nominee purchasers or title holders to purchase U.S. real estate has been on the rise as a method of sanctions evasion. FinCEN's Geographic Targeting Orders (GTOs) in recent years and beneficial ownership rules have aimed to curb this activity.

THIRD-PARTY SERVICE PROVIDERS

The growing role of third-party service providers – such as payment processors, check consolidation, and cash vault service providers – has opened new vulnerabilities in the financial system. These providers are generally not subjected to the same level of regulatory scrutiny as traditional financial institutions.

CYBER-ENABLED METHODS

This newest frontier in sanctions evasion is growing rapidly. Ransomware and theft of high-value digital assets are currently the primary cyber-enabled methods of evading sanctions.[1] Sanctioned actors also conceal their ownership and launder illicit funds through misuse of virtual assets and rapid transfers of funds through various accounts.

Digital assets, including cryptocurrencies, securities, commodities, and derivatives, are increasingly being used to conceal money's true origins and maintain the anonymity of intermediaries. A prominent example is convertible virtual currencies (CVCs), which have become the preferred form of payment for bad actors engaging in various illegal activities, including payments for the ransoms demanded by perpetrators of ransomware attacks.[2] They are also often used to help hide the origins of illicit funds through a complex layering of transactions and/or the use of mixers and tumblers. Mixers and tumblers are mechanisms that break the connection between the sending address and receiving address of a CVC.

An emerging cyber risk can be found in the metaverse, with its evolving parallel economy in which participants are buying digital assets and non-fungible tokens (NFTs), primarily through the use

[1]OFAC Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Sept 21, 2021. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[2]FinCEN Advisory FIN-2019-A003 May 9, 2019, Advisory on Illicit Activity Involving Convertible Virtual Currency

of cryptocurrencies. Generally, online games and virtual worlds transactions are not monitored or registered as closely as their real-world counterparts, and avatars that occupy these spaces perform transactions using digital currencies that have anonymity built into them. While it's true that each party is essentially holding nothing but code, that code has value, and can be easily transferred or exchanged for digital currency, fiat, or for other items that may have greater value. These bad actors could also exploit the trade and sale of these assets by forging NFTs for use and sale across different metaverse platforms, thereby further obfuscating any identifying information.

Metaverse anti-money laundering efforts must therefore be prepared to integrate the best practices and lessons from the real world, such as Know Your Customer (KYC) and monitoring practices, tailored to the risks present in the virtual world.

For example, risk of NFT forgery and theft can be mitigated through user identity control mechanisms such as two-factor authentication and the implementation of an international registry of stolen or fraudulently purchased NFTs, similar to the Art Loss Register utilized in the real-world art market. The metaverse is an emergent and nascent space, so compliance professionals should be prepared to keep up with an ever-complicated landscape, as well as be ready to tackle the innovative ways in which bad actors will disguise and obfuscate their misdeeds.

MONEY SERVICES BUSINESSES

Transactions through both licensed and unlicensed money services businesses can be exploited to obscure beneficial ownership of the transacting parties. Examples of these services include currency dealers, businesses providing traveler's checks, prepaid access, money transmission, currency exchange, check cashing, and money orders.

Significant sanctions-compliance challenges financial institutions face

Financial institutions face a range of challenges in stopping transactions by sanctioned individuals and entities.

RESOURCE-RELATED CHALLENGES:

- Sanctions compliance requires both automated tools and skilled personnel with continuous training.
- Transaction denials or approvals must be made quickly – in real-time – because institutions cannot hold up legitimate transactions.
- Automated systems still struggle to identify non-exact potential name matches, limiting their ability to flag transactions by sanctioned entities. At the same time, ASTs return many false positives that require rapid review by a trained human.
- There is a lack of beneficial ownership information, although this will be eased with FinCEN's beneficial ownership reporting rule.[3] FinCEN issued the proposed rule in December 2021, which could go into effect sometime this year.
- Monitoring some transactions requires wading through complex corporate structures.
- Sanctions lists are constantly being updated, and there are more bad actors now.
- The U.S. regulatory framework tends to lag behind the pace of technology and innovation in both the financial system and sanctions evasion.

[3]FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency, Dec. 7, 2021. https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-beneficial-ownership-reporting-counter-illicit

INDUSTRY-SPECIFIC CHALLENGES:

- Trade and trade finance transactions are challenging to monitor, and doing so is a manual process because this information still comes to banks primarily by fax and email.
- Other industries susceptible to OFAC risk don't have sanctions compliance programs that are nearly as well developed as the financial industry's programs.

Sanctions compliance requires a broad range of costly resources: people, policies, procedures, controls, training, and automated systems.

DIGITAL ASSET CHALLENGES:

- Anonymity is usually explicitly inherent in digital assets and alternative payment systems.
- Transactions involving digital assets, particularly CVCs, often include increased disintermediation more than traditional transactions. This can consist of person-to-person transfers, unhosted wallets, and rapid settlement.

How financial institutions can improve sanctions compliance programs

There are several areas financial institutions can look at to improve the effectiveness of their sanctions program.

1. KNOW YOUR INSTITUTION'S RISK PROFILE.

A financial institution's risk profile should drive many decisions about sanctions compliance programs, such as which sanctions list your AST checks against. Keep in mind that your risk profile may change if you enter new markets, introduce new products or service lines, or even if your client base expands. You may need additional or different systems to monitor for sanctions evasions when that happens. Having an up-to-date risk assessment can help you make better compliance-related decisions.

2. UNDERSTAND YOUR SYSTEM'S CAPABILITIES AND LIMITATIONS.

The biggest issue small and mid-size financial institutions often have with sanctions compliance is that they don't fully understand the capabilities and limitations of their systems. Many larger institutions analyze their system capabilities and limitations and document any limitations and remedial procedures in their Model Risk Management documentation. These systems can be daunting, but you need to know what they're doing – and what they're not doing.

Sanctions screening is largely dependent on the quality and completeness of the information available to financial institutions and there are a number of variables such as the use of common names or name variations, aliases, acronyms, special characters, altered, obscured or missing information that may escape detection.

First, have the capable types of systems and screening in place, including:

- *Sanctions lists direct and non-direct name matching via pertinent data field and fuzzy logic stress testing, respectively*
- *Pattern flagging for potentially illicit transactions*
- *Ways to identify beneficial ownership of entities in a transaction*

- *Well-trained people who understand how to disposition flagged transactions and supporting documentation from the transaction stakeholders.*
- *Leveraging official customs data in KYC and screening processes*
- *Continuous training for front line and compliance personnel*

Second, understand what your systems are doing to catch potential sanctions violations, including:

- *Which customer records and transactions are being screened*
- *What information in the customer and transaction data is not, or cannot, be screened and therefore may require additional or manual review*
- *How they flag accounts and transactions for possible sanction reviews*
- *Which sanctions lists are being used by the systems to screen customers and transactions and how frequently and timely are they updated*
- *Other filtering features such as:*

  Inclusion lists *- internal bank lists to screen for parties not included in the sanction lists that represent risk to the financial institution (i.e., entities from prior investigations, Swift codes from banks located in sanction countries, port cities, International Maritime Organization (IMO) numbers, sanction country names in foreign language, etc.).*

  Exclusion lists *– words and phrases not to be considered in sanction screening used to hasten the impact of false positives (i.e., INC, LLC, CORP, LTD, LTDA, etc.)*

  Behavioral and activity pattern detection *to identify swifts of activity to regions and jurisdictions boarding sanctioned countries*

Your automated screening tool and transaction monitoring systems should be robust, high-quality, and suited to your institution's risk profile. You should also regularly test that these systems are working correctly and detect name variations and current patterns in sanctions evasions.

3. SEARCH AGAINST THE RIGHT SANCTIONS LISTS.

Not all ASTs will screen against all sanctions lists, which may be fine for your financial institution. However, don't assume you only need to screen against the four most common lists (OFAC Specially Designated Nationals and Blocked Persons List, United Nations Security Council Consolidated List, European Union Consolidated Financial Sanctions List, and Her Majesty's Treasury Consolidated List of Financial Sanctions Targets).

Consider adding lists of people known to have evaded or attempted to evade sanctions or lists from the U.S. Department of Commerce and Department of State, such as the Cuba Restricted List.[4] A listing of cities, providences and regions within sanctioned jurisdictions may also help detect transactional activity related to a prohibited country.

Remember that not all ASTs subscribe to all lists, so talk to your provider about which lists are included and consider changing your AST if it makes sense to search lists beyond what it offers. Furthermore, ask your provider to document how often it checks for updates to these lists and how soon these updates are patched into your systems. Your AST should reflect changes to lists as soon as they are available.

Whatever lists you've chosen to use, always use the latest versions. OFAC lists, for example, can update as often as every two weeks. Your system should keep up with OFAC and other list updates.

[4] https://www.state.gov/cuba-sanctions/cuba-restricted-list/

4. SEARCH ALL THE INFORMATION AVAILABLE IN EACH TRANSACTION.

Confirm that your automated systems scan all customer records and relevant wire transfer fields. Don't ignore a field just because the information it contains isn't needed to complete the transaction. These fields could contain information revealing the involvement of a prohibited country or party.

Consider a wire transfer instruction, which has many fields and should contain relevant information about any party involved in the transfer. This might include a third bank that's involved, and your system should be checking that bank's name and business identifier code (BIC) against sanctions lists. A bank's name may be left off a transaction because the bank is on a sanctions list, but the BIC may still be listed and should yield a flag. Furthermore, remember the Department of Commerce maintains a list of prohibited goods and items, which may be described in a wire transfer's non counterparty information field.

5. CONSTANTLY TUNE YOUR SYSTEMS.

Sanctions lists, matching technology, and sanctions evasion techniques are constantly changing, and your systems should be continually evolving, too. Don't be afraid to innovate – OFAC, FinCEN and other regulators have shown tolerance for and encouragement of innovation. While many banks undergo tuning and validation exercises for their OFAC systems to maximize the efficiency and effectiveness of their systems, these systems generally rely on name matching algorithms and tend to generate a large volume of false positive alerts that can require extensive manual review and resolution. In the near future, intelligent automation and artificial intelligence systems may help improve the accuracy of matching systems and lessen the human burden of transaction monitoring.

Innovate, train your people to be aware of risks, be aware of what to look for, and stay on top of trends in both evasion techniques and compliance software.

6. WORK WITH YOUR CLIENTS, ESPECIALLY THOSE IN HIGHER-RISK INDUSTRIES.

While U.S. companies are prohibited from doing business with entities on OFAC's sanctions lists, not all of them have the same compliance requirements as financial institutions. Few industries have compliance programs that are as well developed as those in the financial services industry. Yet, your clients often have more information about the parties involved in a transaction than you do. Collaborate with your clients and develop sanctions risk-mitigation programs.

Some higher-risk industries for sanctions evasion include shipping and other forms of international trade, real estate, cryptocurrency, and art, which tend to attract more illicit financial activity than other industries. Some financial institutions already require clients in these industries to have their own programs to identify, mitigate, and report transactions by sanctioned parties.

You should engage with your clients and set clear institutional expectations detailing your organization's commitment to implementing client-facing processes and requirements that ensure adherence to a sanctions compliance program. These processes could result in your higher-risk industry clients providing additional information or submit to due diligence procedures that are more extensive than those asked of your other lower risk clients.

The next frontiers in sanctions compliance

Financial institutions cannot stop sanctions evasion on their own. Bad actors are increasingly sophisticated, and sanctions evasions schemes more complex. The U.S. sanctions evasion detection approach needs to broaden participation and responsibility to other industries.

The national beneficial ownership registry, provided for in the Corporate Transparency Act, is one step in the right direction in providing greater transparency into the beneficial owners of legal entities.

PUBLIC-PRIVATE COOPERATION

There is consensus that private-public cooperation is required in this area. The more information the government can share with financial institutions, the better industry participants can help prevent sanctions evasion. The proposed OFAC Exchange, for example, would provide the private sector with a single source for information on illicit activity, red flags, and trends in sanctions evasion. Among other benefits, public-private partnerships have the potential to improve the accuracy and usefulness of the data provided to financial institutions, lead to cost efficiencies, improve the effectiveness of anti-money laundering programs, and reduce sanctions evasion.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial intelligence (AI) and machine learning can reduce the number of transactions that must be flagged for human investigation and uncover and mitigate more transactions by sanctioned entities.

For example, financial institutions would benefit from AI tools that can confirm whether someone sharing a name is actually a sanctioned person (e.g., John Doe in Miami vs. John Doe, foreign national). Even more significant potential lies in the ability for computers to learn and recognize new sanctions evasion patterns and flag transactions that match those patterns.

Financial institutions have traditionally been reluctant to innovate in this area because their systems are working for the most part. They may not be willing to rely on automation for these decisions. However, regulators have expressed tolerance and even encouragement for innovation in this sphere in recent years.

It's become increasingly clear that institutions will have to innovate to keep up with the competition from FinTechs and growth in transaction volume and sanctions lists. There is an opportunity for banks to innovate and experiment with intelligent automation and artificial intelligence to lessen the human burden and raise compliance programs' effectiveness.

To keep up with the increased volume and speed of financial transactions and still manage risk appropriately, financial institutions must innovate and invest in new technologies.

TACKLING DIGITAL ASSETS

The U.S. Treasury continues to focus on ways to mitigate sanctions evasion techniques, setting its eye on cryptocurrencies, convertible virtual currencies, and other digital assets. However, experts agree that regulators must better communicate sanctions compliance expectations to businesses in this space. At the same time, experts also request that the Treasury Department should identify and work with relevant gatekeepers within the community as partners in combating sanctions evasion activity.

It's worth noting that, in many cryptocurrency transactions, for example, the transaction will be intermediated by an exchange. The exchange has compliance obligations, including confirming that the transacting parties are not sanctioned entities.

BLOCKCHAINS

Indeed, many aspects of digital assets, including blockchains, can be used to further obscure transacting parties' identities and thus evade sanctions. However, blockchains can also be designed to provide a great deal of transparency and the ability to trace and seize illicit funds transfers.

How? A blockchain records a digital asset's transactions, which must be stored on the blockchain. The blockchain is available to the public, and the community validates its integrity on a periodic basis. While many blockchains are nothing but numbers, it is possible to create blockchains protocols that promote and encourage identifying information of parties associated with crypto transactions. In addition, blockchains can be rich sources of data about financial-activity pattern and several companies in the market now specialize in analyzing blockchain activity.

BRINGING MORE INDUSTRIES UNDER KNOW YOUR CUSTOMER RULES

Real estate and art transactions, the maritime industry, freight forwarders, and digital-currency companies must do more to identify and stop sanctioned transactions, and regulators have acknowledged this. Ideas under consideration include increased incentives for compliance and more robust regulations, supervision, and the development of a culture of compliance at these organizations.

INTERNATIONAL COOPERATION

The U.S. will likely continue to push multilateral forums such as the Financial Action Task Force and other international regulations that will facilitate more transparency in financial transactions. Furthermore, the far-reaching implications of recent national security concerns will likely result in sanctions actions being implemented in concert with allied nations, which will require further strengthening of information and intelligence sharing agreements between international states.

Moving forward

Sanctions compliance programs, and the tools and systems they use, will continue to evolve. And more industries will need to play a bigger part in compliance going forward.

However, whatever the next frontier holds, one thing is clear: Financial institutions will continue to be on the front lines of sanctions compliance efforts.

CONTACT US

Ivan A. Garces, CPA, CFF, CFE, CAMS
Principal & Chair, Risk Advisory Services
Kaufman Rossin
igarces@kaufmanrossin.com

KAUFMAN | ROSSIN

joy is your bottom line

KAUFMAN ROSSIN
cpa + advisors

KAUFMAN ROSSIN
wealth

KAUFMAN ROSSIN
insurance

KAUFMAN ROSSIN
alternative investment services