CHAPTER X

Sanctions Monitorships

Ellen S Zimiles, Patrick J McArdle, Steven McCarthy and Jeremy Robb[1]

The issuance and structure of sanctions monitorships is often similar to other types of monitorships. Regulators and law enforcement agencies are increasingly reliant on independent monitorships as part of enforcement actions following the identification of misconduct or potential corporate crime. The specific nature of sanctions laws and regulations, the binary context of sanctions compliance, the technology systems required to maintain compliance, inconsistencies across geographies and the evolving financial landscape, are unique factors that require specific attention.

This chapter sets forth the legal and historical contexts of sanctions monitorships, recent enforcement actions, the regulatory bodies and other influential organisations involved in the issuance and enforcement of sanctions laws, and specific challenges for institutions placed under a sanctions monitorship.

Legal context of a sanctions monitorship

Sanctions law and regulation are implemented by numerous countries and governing bodies throughout the world. Sanctions can be considered an extension or application of a country's foreign policy, which can be unique to a single country (unilateral sanctions) or jointly applied by multiple countries (multilateral sanctions). Generally, the majority of sanctions are implemented by the United States, the United Nations and the European Union.

---

1 Ellen S Zimiles and Patrick J McArdle are partners, Steven McCarthy is a director and Jeremy Robb is an associate director at Guidehouse.

US sanctions law, dictated by presidential executive orders and through acts of Congress, requires compliance by the following groups and entities:

- US citizens and permanent residents, regardless of present location;
- companies and other entities established under US law;
- people and organisations located within the United States, regardless of origin; and
- branches of US companies and other entities outside the United States.

Sanctions compliance within the United States is applied through the concept of strict liability.[2] All individuals and entities subject to US sanctions law are required to comply regardless of an explicit awareness of non-compliance or a provable intent to evade the law. In the event of a violation or non-compliance with sanctions law, the competent regulatory body or law enforcement agency may choose to pursue civil and criminal action. The extent of penalties often depends on the severity of the infraction and other extenuating circumstances, such as whether the conduct is considered wilful or reckless. In the case of criminal prosecution, penalties against an individual may include a prison sentence, although fines are the most common penalty.[3] In addition to monetary penalties, companies and organisations may be required to commit to remediation efforts or enforcement actions by a regulator or law enforcement, which can include the implementation of business restrictions or the appointment of an independent monitor.

The United States Department of Justice (US DOJ) or other US regulatory bodies may issue various enforcement actions as a result of non-compliance with US sanctions law. These enforcement actions may result from external investigations or proactive disclosures. The Office of Foreign Assets Control (OFAC) and the US DOJ encourage companies to voluntarily self-disclose all potentially wilful violations of the statutes implementing the US government's primary export control and sanctions regimes.[4] If a company (1) voluntarily self-discloses export control or sanctions violations, (2) fully cooperates and (3) remediates the violations appropriately and in a timely manner, there is a presumption that the company will receive a non-prosecution agreement (NPA) and pay a limited

2 Electronic Code of Federal Regulations, 'Appendix A to Part 501 – Economic Sanctions Enforcement Guidelines' (18 Feb. 2020), at https://www.ecfr.gov/cgi-bin/text-idx?SID=ccac94aaa0387efe2a9c3fca2dc5a4ab&mc=true&node=ap31.3.501_1901.a&rgn=div9 (last accessed 1 Mar. 2022).

3 18 U.S. Code § 981; 18 U.S. Code § 982; 18 U.S.C. § 3571(d); 18 U.S.C. § 3572(a).

4 US Department of Justice (US DOJ), 'Export Control and Sanctions Enforcement Policy for Business Organizations' (13 Dec. 2019).

or, potentially, no fine. The US DOJ may enforce criminal resolutions, such as a deferred prosecution agreement (DPA) or guilty plea if the violations exhibit aggravating factors, such as the export of particularly sensitive items, repeated violations, the involvement of senior management and significant profit. In these instances, the US DOJ will issue, or recommend to a sentencing court, a monetary fine, but will not require the appointment of a monitor if the company provides evidence of an established and effective compliance programme being in place at the time of resolution.

The US DOJ continues to evolve its policy and enforcement priorities focusing on white-collar and corporate crime and wrongdoing. In October 2021, the US Deputy Attorney General announced three current priorities and actions the US DOJ is implementing to strengthen the department's efforts to combat corporate crime.[5] The first priority pertains to reinforcing accountability and ensuring all individuals involved in misconduct are held responsible. The second priority focuses on assessing historical misconduct when determining the appropriate resolution, and the record of misconduct speaks to a company's commitment to compliance programmes and instituting the appropriate culture to disincentivise criminal activity. Last, the US Deputy Attorney General explained that the department will modify prior guidance and its stance on the use of corporate monitors. Specifically, she states: 'Instead, I am making clear that the department is free to require the imposition of independent monitors whenever it is appropriate to do so in order to satisfy our prosecutors that a company is living up to its compliance and disclosure obligations under the DPA or NPA.'[6] The US Deputy Attorney General's reinforced efforts to combat corporate crime should serve as a strong indicator to financial institutions and corporations of the likelihood of a required monitorship following the identification of potential criminal activity or significant compliance violations.

5 US DOJ, 'Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime', 08 January 2022, at https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute (last accessed 1 Mar. 2022).

6 id.

Historical context and trends

Recent sanctions enforcement actions and monitorships

Between 2018 and 2021, OFAC issued 69 enforcement actions, including penalties and settlements.[7] Historically, regulators and law enforcement agencies have focused most enforcement actions and monitorships resulting from sanctions violations towards financial institutions. In recent years, however, corporations and financial technology (fintech) companies have been the subject of increased scrutiny and penalties following the discovery of sanctions violations.

Financial institutions

Mashreqbank

In 2021, Mashreqbank agreed to a joint agency resolution with the Federal Reserve System, the New York State Department of Financial Services (NYDFS) and OFAC resulting from confirmed violations of Sudanese sanctions between 2005 and 2009. Overseas branches of Mashreqbank were confirmed to have processed US-dollar denominated funds involving parties subject to OFAC regulations. As part of the cease and desist order, the Federal Reserve System required Mashreqbank to engage an independent external party to perform an annual OFAC compliance assessment for the extent of the terms of the order.[8]

Deutsche Bank AG

In November 2015, Deutsche Bank and the NYDFS agreed to a consent order as a result of the bank's historical dollar clearing transactions processed on behalf of Iranian, Libyan, Syrian, Burmese and Sudanese financial institutions and other entities. As part of the consent order, the NYDFS required Deutsche Bank to engage an independent monitor to perform a comprehensive review of the bank's Bank Secrecy Act (BSA) and anti-money laundering (AML) and OFAC sanctions compliance programmes, policies and procedures.[9]

---

7 US Department of Treasury, 'Civil Penalties and Enforcement Information' (8 Jan. 2022), at https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information (last accessed 1 Mar. 2022).

8 In the Matter of MASHREQBANK PSC Dubai, United Arab Emirates, Order to Cease and Desist (26 Oct. 2021), at https://www.federalreserve.gov/newsevents/pressreleases/files/enf20211109a1.pdf (last accessed 1 Mar. 2022).

9 New York State Department of Financial Services, *In the Matter of Deutsche Bank AG*, Consent Order (30 Jan. 2017), at https://www.dfs.ny.gov/system/files/documents/2020/03/ea170130_deustche_bank.pdf (last accessed 1 Mar. 2022).

Standard Chartered Bank

The Amended DPA between the US DOJ and Standard Chartered Bank (SCB) describes the bank's historical violations, including 'knowingly and willfully conspiring, in violation of Title 18, United States Code, Section 371, to engage in transactions with entities associated with sanctioned countries, including Iran, Sudan, Libya, and Burma' and further states that 'the 2014 DPA Amendment required SCB to retain an independent compliance monitor'.[10]

BNP Paribas

BNP Paribas entered into a plea agreement with the US DOJ on 27 June 2014 for conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA), both sanctions laws imposed by US Congress, through the illegal processing of transactions for countries subject to US economic sanctions. The plea agreement discusses the total forfeiture amount, or fine, levied against BNP Paribas, which takes into account the bank's related settlements imposed by the New York County District Attorney's Office, the Board of Governors of the Federal Reserve System and the NYDFS. In addition, a stipulation of the plea agreement required BNP Paribas to engage a compliance consultant or monitor.[11]

HSBC Bank USA

HSBC entered into a DPA with the US DOJ, which acknowledges the bank's wilful violation of the IEEPA and the TWEA. The DPA required HSBC to retain an independent compliance monitor to evaluate the effectiveness of the bank's internal controls, policies and procedures as regards continuing compliance with the IEEPA, the TWEA and applicable anti-money laundering laws.[12]

---

10 *United States of America v. Standard Chartered Bank*, Notice on Consent of Amended Deferred Prosecution Agreement (9 Apr. 2019), at https://www.justice.gov/opa/press-release/file/1152801/download (last accessed 3 Mar. 2022).

11 US Department of Justice, *United States v. BNP Paribas S.A.*, Plea Agreement (27 Jun. 2014), at https://www.justice.gov/sites/default/files/opa/legacy/2014/06/30/plea-agreement.pdf (last accessed 3 Mar. 2022).

12 *United States of America v. HSBC USA*, Deferred Prosecution Agreement, Attachment B Corporate Compliance Monitor (10 Dec. 2012), at https://www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-executed.pdf (last accessed 3 Mar. 2022).

Financial technology

Fintech companies, which apply technology and other innovative solutions to assist with the delivery of various financial services, continue to be evaluated for their proper adherence to sanctions compliance and regulatory expectations, and remedial action is enforced following the identification of deficiencies or violations.

In December 2020, BitGo Inc, a California-based company that offers its users security and scalability platforms and digital wallet management services, agreed to a monetary settlement with OFAC for sanctions violations as a result of deficiencies regarding its sanctions compliance procedures and internal controls.[13] Specifically, BitGo allegedly processed digital currency transactions on behalf of individuals located in Crimea, Cuba, Iran, Sudan and Syria, the location information being identified through the customers' corresponding internet protocol (IP) addresses.

In February 2021, BitPay Inc, which offers merchant payment processing services inclusive of digital currencies such as bitcoin, and in July 2021, Payoneer Inc, an online money transmitter and provider of prepaid access, both (separately) agreed to settlements with OFAC for sanctions programme violations and programme deficiencies.[14] In both instances, the OFAC settlements explain that BitPay and Payoneer had the means to identify the sanctioned jurisdictions and regions based on available IP address information.

Although, in these instances, OFAC and the US Department of the Treasury did not require the implementation of a monitorship, the settlements serve as a strong indication that fintech companies and the financial services they provide will be subject to ongoing scrutiny and enforcement actions similar to more traditional financial institutions. It should also be noted that the operating model of fintech companies may provide them with data points that are not typically available in the traditional transaction banking context – information such as IP addresses. The regulators have taken the position that transacting institutions must screen all data points readily available for sanctions compliance as evident

13 Department of the Treasury, 'OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions' (30 Dec. 2020), at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf (last accessed 1 Mar. 2022).

14 Department of the Treasury, 'OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions' (18 Feb. 2021), at https://home.treasury.gov/system/files/126/20210218_bp.pdf; 'OFAC Enters Into $1,385,901.40 Settlement with Payoneer Inc. for Apparent Violations of Multiple Sanctions Programs' (23 Jul. 2021), at https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf (web pages last accessed 1 Mar. 2022).

by the Bitgo and BitPay settlements. This should be seen as a warning to others in the industry that failure to incorporate these new expectations could lead to more severe penalties in the future.

Large corporations

ZTE Corporation

ZTE Corporation (ZTEC), a telecommunications company based in China, entered into a plea agreement with the US DOJ in 2017 for conspiring to evade US sanctions law through the illegal shipping of US goods and technology to Iran. The plea agreement states:

> *ZTEC agrees to retain an independent, third-party compliance monitor (the Monitor) to review and assess in a professionally independent and objective fashion ZTEC's processes, policies, and procedures related to compliance with US Export Control Laws, as well as ZTEC's compliance with the terms of this Plea Agreement.*[15]

Huawei Technologies Co Ltd

Huawei, a Chinese multinational technology company, was indicted on charges of knowingly and wilfully conducting business in countries subject to US, UN and EU sanctions, and of efforts to conceal the scope of business activity with sanctioned countries or entities.[16] The US government's investigation of Huawei and the allegations included in the indictment are continuing. With effect from 16 May 2019, the Bureau of Industry and Security (BIS) added Huawei to its restricted entity list as a result of the company's involvement in activities considered contrary to US national security or foreign policy, including violations of the IEEPA through the export, re-export, sale and supply of goods, technology and services (banking and other financial services) from the United States to Iran and the government of Iran.[17] Although Huawei is not currently the subject of a monitorship, the actions taken against the organisation highlight regulators'

---

15 *United States of America v. ZTE Corporation*, Plea Agreement (2 Mar, 2017), at https://www.justice.gov/opa/press-release/file/946276/download (last accessed 3 Mar. 2022).

16 *United States of America v. Huawei Technologies Co., Ltd*, Superseding Indictment (13 Feb. 2020), at https://www.justice.gov/opa/press-release/file/1248961/download (last accessed 3 Mar. 2022).

17 Federal Register, 'Addition of Entities to the Entity List – A Rule by the Industry and Security Bureau on 05/21/2019', at https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list (last accessed 3 Mar. 2022).

increased efforts to seek enforcement actions against corporations, not solely financial institutions. As a result, corporations could also face the prospect of settlements that include provisions for oversight by a monitor for a substantial period.

The enforcers

Legislative bodies, governments and intergovernmental organisations all implement various forms of sanctions law, resolutions or restrictive measures. Separately, in most cases, related government branches, regulatory bodies and law enforcers are responsible for the enforcement and monitoring of sanctions compliance. The primary enforcers of sanctions measures include the United States, the United Nations, the European Union, as well as other countries and influential organisations.

United States

OFAC, BIS, other financial regulators such as the Office of the Comptroller of the Currency, the Federal Reserve Bank and state-level regulators, such as the NYDFS, each have a role in the monitoring of sanctions compliance. OFAC, as part of the Department of the Treasury, maintains the Specially Designated Nationals and Blocked Persons lists, which identify individuals, companies and other entities deemed restricted, requiring activity to be blocked or frozen. Within the Department of Commerce, the BIS is responsible for the Denied Persons List, a catalogue of individuals who are denied export privileges, and for the Export Administration Regulations, which apply export controls to specific commodities, technology, software and other items.

The NYDFS implemented its 504 Rule pertaining to Transaction Monitoring and Filtering Program Requirements and Certifications following prior investigations into institutions regulated by the NYDFS and various identified deficiencies. The 504 Rule aims to clarify the required components of a transaction monitoring and filtering programme. Further, it specifically requires management to certify that a filtering programme is reasonably designed to interdict transactions prohibited by OFAC, similar to the requirements of The Sarbanes–Oxley Act of 2002.[18]

18 New York State Department of Financial Services, Superintendent's Regulations, 'Part 504 Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications' (1 Jan. 2017), at https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=Ie3242420479311e6b718fc8ac47ba487&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default) (last accessed 10 Mar. 2022).

United Nations

The United Nations enacts sanctions regulations through resolutions, and the UN Security Council sets the specific criteria for targeting individuals and entities. The UN Security Council is composed of 15 member countries, with each member participating or voting to enact sanctions resolutions. Member States of the United Nations are each obliged to adopt and comply with the UN sanctions resolutions but may also create their own laws and regulations and enforcement bodies.

European Union

The European Union imposes sanctions law through restrictive measures developed by the European External Action Service and agreed to by the Council of the European Union. The European Union implements all UN-issued sanctions resolutions and EU Member States are required to enact individualised legislation for sanctions monitoring and enforcement, including penalties for violations.

Other nations

Various other countries enact sanctions law and compliance requirements and establish local authorities to oversee enforcement. The following are some examples:

- *United Kingdom*: The Office of Financial Sanctions Implementation (part of HM Treasury) establishes and administers sanctions.
- *Australia*: The Department of Foreign Affairs and Trade enacts general sanctions policy.
- *Singapore*: The Monetary Authority of Singapore administers financial sanctions.

Influential organisations

Several notable organisations have taken steps to further develop principles and guidance to aid in anti-money laundering, terrorist financing and sanctions compliance.

Financial Action Task Force

In 1989, seven countries came together to create the Financial Action Task Force (FATF) with the primary goal of developing recommendations on international standards to combat money laundering and terrorist financing. The FATF has grown to 35 Member States, each required to adhere to the FATF recommendations. Additionally, the FATF publishes Mutual Evaluation Reports, which evaluate a country's adherence to the FATF recommendations.

The Wolfsberg Group

The Wolfsberg Group, an international organisation composed of 13 global banks, develops and publishes guidance for global banks on the framework and best practices for managing and combating financial crime risk.

The legal requirements

As discussed above, the United States, the United Nations and the European Union have implemented more numerous and comprehensive sanctions regimes than other countries or intergovernmental bodies. Upon implementation of a law or restriction, various regulatory bodies, such as OFAC, are tasked with enforcement.

In the United States, the President may enact sanctions regulations through Acts of Congress or Executive Orders. The UN Security Council implements sanctions or resolutions, and all Member States are expected to adopt the passed resolutions. Last, the European External Action Service prepares restrictive measures to which Member States are expected to adhere.

Unique challenges of sanctions monitorships and compliance

Financial institutions under a sanctions monitorship

Financial institutions under a sanctions monitorship encounter several challenges to comply with the terms of a monitorship and regulatory requirements. From a general perspective, unique aspects of a sanctions monitorship include (1) the global scope versus the regional scope of the remediation, (2) the level of remediation efforts and regulator involvement, (3) the effect on 'business as usual' of monitorship requirements and (4) system enhancements and technology changes. Specific challenges also include data issues, inconsistent or conflicting regulation of sanctions law against certain countries, and the requirements of a DPA or consent order may be more restrictive than the law.

Global versus regional scope

The scope of the monitorship presents a challenge to financial institutions based on the size of the institution, the geographies within which it operates, the number of customers, the products and services offered and the delivery channels. For example, sanctions violations may originate from one region or branch of a financial institution, leading to localised remediation efforts of the regional sanctions compliance programme. A financial institution with a more expansive footprint and a global presence may require enhancements to the global sanctions compliance programme, and compliance elements unique to each region. It is imperative that regional sanctions personnel are properly trained on the requirements of the global sanctions compliance programme and on the sanctions laws

of the jurisdictions where the financial institution conducts business or processes transactions. In addition, changes and enhancements made to a global sanctions compliance programme may require implementation in the applicable regional sanctions compliance programmes.

Remediation efforts and regulator involvement

Monitorships exhibit varying levels of involvement by multiple enforcement bodies and consulting firms. For example, a financial institution may be simultaneously complying with multiple DPAs or consent orders involving more than one enforcement body (such as the NYDFS, the US DOJ or, in the United Kingdom, the Prudential Regulatory Authority). Depending on the scope of the engagement or applicable conflicts of interest, the enforcement bodies may engage different consulting firms to carry out the work. As such, the financial institution may handle requests for information and meetings from multiple firms, resulting in potential duplication of efforts and increased burden on sanctions personnel. Additionally, the enforcement body's level of direct involvement may vary. For example, an enforcement body may be satisfied with receiving updates from the monitor on the status of the engagement, while another may prefer to have regular meetings itself with the financial institution or submit special requests in addition to those made by the monitor.

Regulatory and jurisdictional conflicts

Financial institutions may also encounter potential conflicts between the requirements of a DPA and the application of sanctions laws across various countries. Specifically, the requirements of the applicable DPA or consent order may be more restrictive than the governing laws of the jurisdiction where the financial institution resides or conducts business. As such, the financial institution may be required to implement additional programme enhancements or compliance measures beyond those necessary to comply with regional sanctions laws, which may necessitate an increase in compliance budget or personnel. Further, the application of sanctions laws against a particular country may vary depending on the jurisdiction. Specifically, sanctions implemented against a country such as Cuba by the United States may not be honoured by other countries and could cause a conflict for financial institutions with customers transacting with both Cuba and the United States.

Balancing 'business as usual' with monitorship requirements

Financial institutions working with an appointed monitor to oversee compliance with the terms of a DPA or consent order face the unique challenge of balancing 'business as usual' responsibilities with the additional work required to comply with

monitor, regulator or law enforcement requests. Specifically, in addition to day-to-day responsibilities and requests from the monitor, the sanctions or compliance teams are often responding to requests from internal audit or compliance assurance. Further, the monitor may submit a substantial number of document requests, and schedule meetings and interviews with sanctions personnel to gain a better understanding both of the levels of knowledge and expertise of the staff and of the sanctions compliance process in place at the financial institution. These simultaneous requests can place a significant strain on resources, specifically the sanctions personnel responding to requests for documentation and attending meetings with the monitor and those responsible for the applicable internal compliance functions.

The monitor may also identify findings and related recommendations to improve the financial institution's sanctions compliance programme, including enhancements to policies and procedures, improvements to processes or programme documents, and the addition or reassignment of sanctions personnel. The increased workload to comply with the terms of the monitorship, remediate any findings and implement enhancements to the programme may require the financial institution to hire additional full-time staff or contract work out to external firms.

It is imperative that the business or corporate functions of the financial institution remain aware of the challenges being faced and the amount of work and financial commitment needed to comply with the terms of the monitorship. The sanctions compliance team should provide regular updates to the governance oversight committee, senior leadership and board of directors on the progress of the monitorship and any significant changes required to remediate the monitor's findings. Without full commitment from the financial institution to approve additional funding or increase staff, the sanctions compliance team may struggle to balance 'business as usual' with the requirements of the monitorship, posing additional compliance risk to the institution.

Data, sanctions technology and personnel

Data challenges

Data presents a challenge to financial institutions in complying with sanctions laws as the volume and format of available data varies across institutions and jurisdictions. Frequently, data sources can be truncated, incomplete and disjointed across multiple systems or platforms within the institution, making it difficult to maintain real-time watch list screening practices. In addition, the data must be screened against state, federal and international watch lists, depending on regulatory requirements. Further, institutions with a global presence face the challenge of differing data privacy laws and translation or transliteration processes. Finally, the volume of data in an organisation can further complicate sanctions screening. The difficulty in

monitoring the flow of payments increases as an institution expands its customer base and the products and services offered. Specific challenges include customer onboarding and identity verification, transaction screening and watch list updates.[19]

System technology

Additional challenges for financial institutions facing sanctions monitorships include the implementation of the enhancements recommended by the monitor. These often involve enhancements to sanctions screening technology, changes to, or the implementation of, case management systems and improvements to list management processes. Implementing system changes or new technologies presents additional risk as system down time can lead to a backlog of required regulatory filings, such as potential circumvention attempts and voluntary self-disclosures. Further, changes to sanctions screening technology and system settings may increase the number of sanctions alerts and cases requiring review and possible escalation.

During the covid-19 pandemic, several jurisdictions have noted an increased use of new and emerging information technology (IT) tools to assist with AML and the prevention and supervision of terrorism financing, specifically in respect of sanctions screening. In addition, new systems have been developed utilising blockchain technology.[20] The use of newly developed systems and technology may pose an increased risk of potential sanctions programme violations if the systems are not fully tested or calibrated sufficiently to identify possible sanctions hits. Users of new technology should endeavour to educate their regulators on their system's process and output so that the agencies are more comfortable with its use.

Sanctions personnel and training

System enhancements and the implementation of new technology requires financial institutions to conduct supplementary training for all sanctions personnel as well as the required formal compliance training programme. The training ensures that all members of staff are deploying the sanctions screening technology in the proper manner and serves as an important control in the mitigation of sanctions compliance risks to which the financial institution may be exposed. In addition,

19 Computer Services, Inc, 'The 4 Major Challenges of Real-Time Sanctions Screening' (21 Sep. 2017), at https://www.csiweb.com/resources/blog/post/2017/09/21/the-4-major-challenges-of-real-time-sanctions-screening (last accessed 3 Mar. 2022).

20 Council of Europe Typologies Report, 'AML/CTF Supervision in Times of Crisis and Challenging External Factors' (25 Jan. 2022), pp. 10–11, at https://rm.coe.int/typologies-report/1680a54995 (last accessed 3 Mar. 2022).

a monitor may make recommendations to augment or reduce the number of sanctions compliance personnel, based on the appropriateness of roles and responsibilities, sanctions experience and industry knowledge. The proposed changes in roles or responsibilities might result in staff attrition or a heavier workload for the sanctions team.

Maintaining sanctions compliance

Financial institutions face continuous challenges in maintaining compliance with local and international sanctions laws. Specifically, the following can affect a financial institution's sanctions compliance programme.

Evolving sanctions regulation and regimes

Sanctions regulation and regimes are continually evolving, creating a moving target for financial institutions striving to achieve compliance with regulatory standards. Effectively monitoring these changes and staying informed about the global political climate mitigates the risk inherent to financial institutions posed by these changes. Methods of staying current include requiring vendors to provide updated lists, monitoring government websites through subscriptions and creating tailored news alerts. In addition, consulting external sanctions experts or counsel can ensure that an institution stays aware of sanctions developments. Sanctions counsel can actively track pending sanctions legislation and provide real-time advice on developments.[21] Financial institutions must also remain diligent in updating sanctions-related policies, procedures and process documents to reflect these changes, train applicable personnel on any developments affecting their day-to-day responsibilities and rescreen any customers who may be affected by the regulatory changes.

Jurisdiction or extraterritoriality issues

It is critical that financial institutions maintain continuous awareness of both domestic and international sanctions requirements. Sanctions measures and requirements for compliance can be complex in nature and the level of cooperation between jurisdictions varies. In certain circumstances, economic sanctions imposed by one jurisdiction may result in measures being imposed against entities located in another country. Examples include the scope and application of the

21 Financier Worldwide, 'Global sanctions – compliance and enforcement trends' (Oct. 2017), at https://www.financierworldwide.com/global-sanctions-compliance-and-enforcement-trends#.Xk1v9yhKjGi (last accessed 3 Mar. 2022).

TWEA and IEEPA.[22] In addition, some economic sanctions may conflict with the sanctions laws enacted in another country, creating a challenge for financial institutions conducting business in both countries as to which sanctions laws they are required to follow. Further, some jurisdictions have enacted blocking statutes designed to shield entities in a particular jurisdiction by disallowing the recognition of certain extraterritorial sanctions imposed by other countries. The European Union established one such blocking statute, which nullifies US sanctions against commercial trade with Iran.[23]

Further, many sanctions measures are not absolute in their application and include the possibility of exemptions. Entities in the United States, for example, may apply for specific licences for (1) the release of blocked funds, (2) travel under specified conditions to jurisdictions that the sanctions measures would otherwise prohibit or (3) exporting certain commodities that support medical and agricultural needs in sanctioned jurisdictions.[24] The myriad complexities in the application and enforcement of sanctions efforts across jurisdictions can present challenges in maintaining an effective sanctions compliance programme.

Global trade processes and data privacy laws

In addition to evolving regulations and jurisdictional conflicts, international trade finance continues to operate using outdated technology and antiquated processes that create greater risk of sanctions evasion. Specific examples include (1) trade agreements written before the emergence of digital commerce, (2) transactions accompanied by large amounts of paperwork and (3) trade financing that depends on traditional banking methods.[25] A large portion of the trade industry is still based on paper documents and antiquated processes that slow international commerce and have a significant effect on the economy. Specifically, drawbacks of the global trade process include (1) trucks and containers standing idle at ports, (2) cash

22 International Bar Association, 'United States extraterritoriality: European Union sovereignty at stake https://www.ibanet.org/article/CF85E59E-6564-4AA3-9408-3F47C6449C9D (last accessed 10 Mar. 2022).

23 European Commission, 'Updated Blocking Statute in support of Iran nuclear deal enters into force' (6 Aug. 2018), at https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4805 (last accessed 3 Mar. 2022).

24 US Department of the Treasury, 'OFAC License Application Page' (23 Jul. 2018), at https://home.treasury.gov/policy-issues/financial-sanctions/ofac-license-application-page (last accessed 1 Mar. 2022).

25 World Economic Forum, 'These 5 technologies have the potential to change global trade forever' (6 Jun. 2018), at https://www.weforum.org/agenda/2018/06/from-blockchain-to-mobile-payments-these-technologies-will-disrupt-global-trade/ (last accessed 3 Mar. 2022).

flow tied up in goods awaiting the production of trade documents and (3) a lack of visibility and inventory status.[26] Further, missing documentation, inadequate global location tracking and diluted or forfeited data pose daily challenges to sanctions compliance efforts.

In addition, data privacy laws differ across jurisdictions. In certain countries, such as Zimbabwe and South Korea, the data privacy laws limit or restrict the provision of confidential data across jurisdictions. Further, colleagues working within the same institution with a global presence may not be permitted to share information unless they are both physically present in the jurisdiction where the data is stored. Lack of access to certain information poses a challenge to financial institutions in complying with international sanctions laws and opens up the institution to additional risks of a sanctions violation.

Digital assets

Digital assets, such as cryptocurrencies, present challenges to financial institutions in complying with regulatory sanctions requirements owing to the wide array of products and services, and the thousands of cryptocurrencies, currently in circulation. The complexity of cryptocurrency makes it difficult for financial institutions to identify and control inherent risks, making cryptocurrencies attractive to entities in sanctioned countries, such as Iran and Cuba. Although many cryptocurrency products are traceable and regulated in certain jurisdictions (such as Switzerland and the United States) by agencies such as the Financial Crimes Enforcement Network, sanctioned entities can gain access to cryptocurrencies through non-traditional means, such as the dark web, or cryptocurrency mining, which creates anonymity for users, and further rely on mixers or tumblers to obscure the source of funds.[27] This anonymity increases the difficulty of identifying circumvention attempts by those sanctioned entities.

Furthermore, cryptocurrency and other digital asset transactions introduce additional identifying information, including digital wallet and IP addresses, and other forms of geolocation information unique to digital or online activity. The availability of this type of information introduces additional screening

26 IOTA Foundation, 'The Challenges Facing Today's Supply Chains' (20 Dec. 2018), at https://blog.iota.org/the-challenges-facing-todays-supply-chains-aaa9d3d9fc6d (last accessed 3 Mar. 2022).

27 Cryptocurrency tumblers or mixing services are utilised to mix potentially identifiable, illicit or tainted cryptocurrency funds with others, in order to obfuscate the fund's original source or ownership. See Ciphertrace, 'Mixers, Tumblers, Foggers' (7 Feb. 2022), at https://ciphertrace.com/glossary/mixer-tumbler-fogger/ (last accessed 3 Mar. 2022).

and due diligence requirements for all institutions and organisations involved. In November 2018, OFAC added the first two cryptocurrency addresses to its Specially Designated Nationals (SDN) list, which were found to be associated with individuals responsible for exchanging the proceeds of a ransomware attack.[28] In October 2021, OFAC published guidance regarding virtual currencies that details regulatory expectations for sanctions compliance in the evolving industry.[29]

The instances and methods of cryptocurrency adoption continue to develop and evolve, which can make sanctions compliance even more challenging. In September 2021, El Salvador became the first country to adopt bitcoin as an official currency with legal tender allowing the conversion of bitcoin to US dollars, El Salvador's official currency. Shortly after this, however, the International Monetary Fund delivered recommendations that El Salvador rethink the crypto adoption and issued specific warnings that the costs of El Salvador's adoption of bitcoin outweigh any benefits, and introduces considerable risk to financial stability, market stability and consumer protections.[30]

The future

Artificial intelligence (AI) is the future for sanctions and BSA/AML compliance, but it is also a new area of focus for regulators and law enforcement. Financial institutions investing in AI implementation to improve efficiencies should be fully versed in the solution so that it can be explained easily to regulators and law enforcement. The AI should also be customisable to account for the dynamic nature of economic sanctions, as it appears that governments are amenable to an expanded use of economic sanctions. Further, the use of AI will require the introduction of a quality assurance (QA) component by sanctions personnel. In addition to the time spent to review the output of AI, the QA review introduces further risk of potential human error to the process.

---

28 US Department of the Treasury, Press release, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses' (28 Nov. 2018), at https://home.treasury.gov/news/press-releases/sm556 (last accessed 3 Mar. 2022).

29 US Department of the Treasury, Office of Foreign Assets Control, 'Sanctions Compliance Guidance for the Virtual Currency Industry' (Oct. 2021), at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf (last accessed 3 Mar. 2022).

30 Bitcoin.com, 'IMF Tells El Salvador: Costs of Making Bitcoin Legal Tender Exceed Potential Benefits' (30 Jan. 2022), at https://news.bitcoin.com/imf-tells-el-salvador-costs-of-making-bitcoin-legal-tender-exceed-potential-benefits/ (last accessed 3 Mar. 2022).

Sanctions technology can automate repetitive and menial tasks to make a financial institution's sanctions compliance programme more efficient. If not properly tuned or maintained, however, it could magnify inaccuracies by repeating the same fault on multiple occasions. Financial institutions should conduct periodic model and data validation testing to ensure that the system performs exactly as intended.

Conclusion

Law enforcement and regulatory bodies are becoming more comfortable with the inclusion of an independent body as part of a settlement to ensure their remediation requirements are met. Specifically, regulators and law enforcement agencies appear to be increasing the penalties and frequency of enforcement actions, including the use of monitorships, for economic sanctions violations. Financial institutions and corporations should prepare for the possibility of receiving a monitor as part of a settlement. If this is the case, the institution needs to plan and prepare to manage the process as smoothly as possible. The institution and its staff will be challenged to maintain business as usual while also responding to requests from the monitor, regulators and internal or external auditors. Financial institutions, fintech companies and corporations can all benefit from evaluating whether their current programme complies with sanctions law and regulation, keeping in mind the continuing and evolving complexities of sanctions compliance. Further, sanctions technology and AI may be a focus for regulators and law enforcement agencies in future sanctions monitorships, as the use of AI becomes more prevalent in financial institutions and sanctions compliance programmes.

CONTACTS & BIOGRAPHY SECTION

Guidehouse

685 3rd Avenue, 14th floor
New York, NY 10017
United States
Tel: +1 646 227 4200
ellen.zimiles@guidehouse.com
patrick.mcardle@guidehouse.com
steven.mccarthy@guidehouse.com
jeremy.robb@guidehouse.com
www.guidehouse.com/financialservices

Firm description

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency and technology-driven innovation. Across a range of advisory, consulting, outsourcing and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 12,000 professionals in over 50 locations globally.

Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit www.guidehouse.com/financialservices.

Patrick J McArdle

Guidehouse

Patrick J McArdle, a partner in the global investigations and compliance practice, has more than 25 years of experience in regulatory compliance, consulting and law enforcement. He specialises in Bank Secrecy Act (BSA) and anti-money laundering (AML) compliance, fraud prevention and forensic accounting investigations.

Patrick was a regulatory enforcement investigator, which required him to conduct highly sensitive and complex specialised investigations involving violations of bank regulations, illegal activities and suspicious transactions. This work required Patrick to develop and test numerous BSA/AML compliance programmes.

Patrick has led numerous fraud investigations involving financial statement fraud, embezzlements, inventory and receivable manipulations, bid rigging and kickback arrangements across a variety of industries. He has also worked as a financial investigator for a local prosecutor's office, focusing on gathering and compiling various financial records and statements for trial. This unique blend of experience makes Patrick a valuable resource for a wide range of regulatory and fraud investigations.

Steven McCarthy
Guidehouse

Steven McCarthy is a director in Guidehouse's global investigations and compliance practice. He has 15 years of extensive experience in providing regulatory compliance, advisory and investigative services to private and public sector clients. He has expertise in performing services on behalf of financial institutions relative to compliance with the Bank Secrecy Act (BSA), anti-money laundering (AML) regulations, the USA PATRIOT Act and Office of Foreign Assets Control (OFAC) guidelines.

Steven manages a large-scale independent audit engagement resulting from a class action settlement involving a public education school system. He has assisted in several BSA/AML and OFAC compliance reviews and a variety of AML investigation, gap analysis and independent testing engagements for financial institutions, including domestic and foreign banks, broker dealers and investment advisers. Steven also has experience in assessing the BSA/AML and sanctions programmes of global financial institutions to ensure adherence with applicable laws, regulations and industry better practices, to identify deficiencies in the programme and to recommend corrective measures.

Jeremy Robb
Guidehouse

Jeremy Robb is an associate director in the Guidehouse New York office. Within the global investigations and compliance practice, Jeremy has more than six years of experience in performing advisory services for clients, including compliance with the Bank Secrecy Act and anti-money laundering regulations, and Office of Foreign Assets Control sanctions regulation and industry best practices. Jeremy has extensive experience with financial institution monitorships and independent assessments, of both US and international regulatory standards. Jeremy has provided analytical and investigative work during the monitorship of an international

financial institution, which included a global assessment of compliance with US economic sanctions. Jeremy is recognised as a certified global sanctions specialist by the Association of Certified Anti-Money Laundering Specialists.

Ellen S Zimiles
Guidehouse

Ellen S Zimiles is Guidehouse's financial services advisory and compliance segment leader and has more than 30 years of litigation and investigation experience, including 10 years as a federal prosecutor in the US Attorney's Office for the Southern District of New York.

Ellen is a leading authority on anti-money laundering programmes, corporate governance, foreign and domestic public corruption matters, regulatory and corporate compliance and fraud control. Ellen has worked with many financial institutions preparing for regulatory exams and has extensive experience in developing remediation programmes, serving as a regulatory liaison and independent monitor, as well as advising organisations that are the subject of a monitorship.

Ellen was engaged by a multinational financial institution as an independent monitor to conduct a compliance assessment of its Bank Secrecy Act, anti-money laundering and sanctions programmes in response to a regulatory consent order and deferred prosecution agreement with the New York State Department of Financial Services, the US Department of Justice and the District Attorney of New York County. Additionally, Ellen has led numerous independent consultant engagements for regulators related to sanctions and financial crime.

Since 2008, Ellen has led a team serving as independent auditor to monitor compliance with the terms of a settlement agreement between the NYC Department of Education and the parents of children entitled to special education services.

With the approval of the Federal Highway Administration, Ellen was engaged by a global supplier of commercial highway products to serve as an independent monitor for a three-year period. The monitorship was the result of a settlement agreement following a civil judgment pursuant to the False Claims Act.