Evolving Sanctions Circumvention Techniques and the Role of Audit

White Paper for Advanced CAMS - Audit certification

CHAN Yiu Lai, Charles
February 2020
# Table of Contents

**Abstract** ........................................................................................................................................... 2  
**Acknowledgements** ......................................................................................................................... 2  
**Background and Introduction** ........................................................................................................... 3  
**What Are Sanctions?** ....................................................................................................................... 4  
**What Is Sanctions Circumvention?** .................................................................................................... 5  
**Evolving Sanctions Circumvention Techniques** .................................................................................. 5  
**Case Studies** ..................................................................................................................................... 20  
**How Can Financial Institutions Face This Evolving Situation?** ..................................................... 25  
**Conclusion** ......................................................................................................................................... 29  
**References** ......................................................................................................................................... 30
Abstract

This whitepaper is not aiming to encourage sanctions circumventions, instead, to highlight evolving sanctions circumventions techniques by targeting weaknesses and room for improvement in sanctions compliance programs. This white paper also highlights the role of audit in sanctions compliance in handling new sanctions circumventions methods.

Acknowledgements

Sincere gratitude is hereby extended to the following people who never ceased in helping until this paper was structured and finalized: The mentor Marc, the thesis adviser, for the unwavering guidance; for the unwavering moral, emotional, and financial support of my wife Jacqueline, family, and friends, including Jing Jing LEE, Binita SHAH, Phitchayada SUWANNAKOM in this Advanced CAMS Audit program. My utmost appreciation goes to almighty God for divine intervention in this white paper.
Background and Introduction

Sanctions regulatory landscape is ever-changing; sanctioned entities are also ever-evolving their ways to circumvent sanctions regulations to use international financial systems for their “business.” Financial institutions are always preventing breaches in sanctions regulations to avoid facing significant fines,\(^1\) civil and criminal prosecution,\(^2\) revocation of banking licenses,\(^3\) banning from entering certain types of financial transactions, and not engaging in new client relationships, all of which could cause a destructive consequence to a financial institution’s business and operations.

The objective of this paper is twofold. First, to identify sanctions circumvention techniques utilized by sanctioned entities (e.g., terrorist organizations, their fund contributors, governments, companies; or individuals who engage in proliferation of weapons of mass destruction, or violate international norms of behaviour). As sanctioned entities are required to use the financial system to fund their operations or receive proceeds, they need to find different ways to inject their funds by circumventing existing sanctions compliance programs.

Since there are new, enhanced, and emerging techniques for sanctioned entities to circumvent the existing sanctions compliance programs, this paper also aims to explore what bank internal auditors could consider and the measures they could take for identifying these new circumvention techniques through the existing sanctions compliance program (SCP) of the financial institution.

---

\(^1\) OFAC’s List of Enforcement actions: https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx
OFAC’s enforcement guidelines: https://www.ecfr.gov/cgi-bin/text-idx?SID=ccac94aaa0387efe2a9c3fca2dc5a4ab&mc=true&node=ap31.3.501_1901.a&rgn=div9


\(^3\) BNP Paribas’s case in 2014: https://www.reuters.com/article/us-bnp-paribas-settlement/u-s-imposes-record-fine-on-bnp-in-sanctions-warning-to-banks-idUSKBN0F52HA20140701
What Are Sanctions?

Sanctions could be an economic international policy tool, or simply, a political tool when some unwanted behaviour of a country (e.g., Liberia, in relation to Charles Taylor), group or entity (e.g., terrorists), or an individual needing to change without using armed conflict. Sanctions aim to force the target country, firm, or individual to comply with the goal of the imposing country or of the supranational bodies, such as the United Nations (U.N.)\(^5\), or law enforcement agencies, such as the United States of America’s Office of Foreign Assets Control (OFAC),\(^6\) the European Union\(^7\) (EU), or smaller jurisdictions including Taiwan or Hong Kong.\(^8\)

Financial institutions are involved in this international game of sanctions as one of the intermediaries dealing with international trade and payments. By not complying with sanctions regulations, financial institutions may be subject to serious consequences.


Meanwhile, from recent sanctions actions from United States President Donald Trump on Iran also addressed to use sanctions instead of armed forces to Iran: https://edition.cnn.com/2020/01/08/politics/trump-iran-sanctions/index.html

\(^5\) For example, U.N. sanctions on DPRK: https://www.un.org/securitycouncil/sanctions/1718

\(^6\) Ibid. (1)

\(^7\) See list of European Union’s sanctions regime: https://www.sanctionsmap.eu/

\(^8\) For example, Taiwan maintains their sanctions regime under the Counter-Terrorism Financing Act under Ministry of Justice, which their sanctions regime is based on "international treaty or convention in connection with Terrorist Financing prevention so requires or such is necessary to implement international cooperation or United Nations resolutions": https://www.mjib.gov.tw/userfiles/files/35-%E6%B4%97%E9%8C%A2%E9%98%B2%E5%88%B6%E8%99%95/%E6%B4%97%E9%8C%A2%E9%98%B2%E5%88%B6%E8%99%95-EN/2.pdf

For Hong Kong’s sanctions regime, the Hong Kong Monetary Authority requests financial institutions maintain sanctions a database of individuals and entities designated under the United Nations Sanctions Ordinance (UNSO) and United Nations (Anti-Terrorism Measures) Ordinance (UNATMO) for customer and transaction screening purposes. The Commerce and Economic Development Bureau is responsible for maintaining lists of designated individuals and entities under the UNSO, while the Security Bureau maintains lists of designated individuals and entities under the UNATMO: https://www.hkma.gov.hk/eng/key-functions/banking/anti-money-laundering-and-counter-financing-of-terrorism/sanctions-related-notices-updates/
such as heavy fines\textsuperscript{9}, revocation of banking license\textsuperscript{10}, sanctions\textsuperscript{11} (especially from US OFAC).

**What Is Sanctions Circumvention?**

Sanctions circumvention, from a dictionary definition, is an action of overcoming the problem of sanction violation in a clever and surreptitious way. Circumvention is also an action employed by a sanctioned entity to avoid being discovered by law enforcement agencies or financial institutions. Circumventions are counter-sanctions measures taken by sanctioned entities, individuals, or even countries to give the appearance of normal operations, by leveraging the weaknesses and vulnerabilities of existing sanctions regimes.

**Evolving Sanctions Circumvention Techniques**

As per the Chinese saying, “Mastering the stick, but aiming for the yard” (道高一尺,魔高一丈), when some countries impose a new, more restricted sanctions program, there will always be new sanctions circumvention methods to attack the weakness and vulnerabilities of new sanctions regimes. (Actually, this will be an endless game unless the world is totally at peace, which is an impossibility.)

Thus, as mentioned, since supranational bodies or countries are keener to use more restricted sanctions regimes, sanctioned entities are also improving themselves by using evolving sanctions circumvention techniques by attacking the weakness and vulnerabilities of the sanctions regimes. Some of the evolving techniques may be

\textsuperscript{9} Ibid. (1)
\textsuperscript{10} Ibid. (1)
\textsuperscript{11} OFAC sanctions against Bank of Kunlun in China and Elaf Bank in Iraq in 2012 for business with designated Iranian banks under the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 in connection with Iran’s weapons of mass destruction programs or its support for international terrorism:
OFAC also sanctioned several Lebanon-based financial institutions in 2019 due to their providing of financial services to Hizballah as Specially Designated Global Terrorist:
simple but very effective as there is no clue for financial institutions, law enforcement agencies, or regulators to identify such payments, clients, or firms that are sanctions related.

A. Concealment of ultimate beneficial ownership

From OFAC’s recently released advisory document, “A Framework for OFAC Compliance Commitments,” improper due diligence of customers or clients (including beneficial ownership, business dealings) is one of the root causes of breakdowns or deficiencies in a sanctions compliance program. The Financial Action Task Force (FATF) document, Concealment of Beneficial Ownership, also highlights this:

The ownership and control of illicit assets, and the use of legal structures to conceal them, has been the subject of increased global attention in recent years. The leak of confidential information from two large international law firms responsible for the establishment of complex international corporate structures in 2015 and 2017 has increased public awareness of the way in which legal structures can be used to conceal wealth and illicit assets.

On the other hand, OFAC also stressed entity ownership since 2008 from their 2014 guidance on the 50% rule. Specifically, OFAC stated that:

Entity individually or in the aggregate, directly or indirectly owns more than 50% or more by one or more blocked persons is itself considered to be a blocked person.

Hence concealment of beneficial ownership could prevent detection and frustrate investigations. Similar to what criminals did in using legitimate

---

12 See treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf
14 Panama papers leak in 2015: https://www.icij.org/investigations/panama-papers/
15 Paradise papers leak in 2017: https://www.icij.org/investigations/paradise-papers/
16 From OFAC’s FAQs: https://www.treasury.gov/resource-center/faqs/Sanctions/Documents/faq_all.html
corporate structures to hide illicit source of assets, sanctioned countries and entities also need to hide the original sources of funds (which may have been derived from normal business operations). Thus, concealment of beneficial ownership is always one of the major methods used by sanctioned entities to hide the ownership information as well as the source of wealth and funds.

Examples of methods of concealment of beneficial ownerships include:

1. Generating complex ownership and control structures
   This method disguises the beneficial ownership by distancing the ultimate beneficial owner in using various legal structures and arrangements, by adding numerous layers of ownership between the ownership and control structures and the ultimate beneficial owner. The ultimate beneficial owner uses both direct and indirect ways to maintain the control of assets. In using various legal arrangements and in different jurisdictions, the ultimate beneficial owner could prevent detection and frustrate investigations by making the ownership structures as complex as possible and the actual percentage of ultimate beneficial ownership hard to calculate. While this method is not only used by criminals or sanctioned entities, large international corporations and high net worth individuals are also using the same way to distinguish different business lines and activities.

However, only the complex structure method is not quite as useful to obfuscate financial institutions. During the account opening or review process, financial institutions always require customers to provide the entire ownership chain towards persons as the ultimate beneficial owners, and require all sorts of documentation including company registry records, certificate of incumbency (for offshore incorporated companies including British Virgin Islands, Cayman Islands, Samoa, or Panama, etc.), and identification documents for ultimate beneficial owners. Also the percentage of ultimate beneficial ownership on an entity is lower than 50%, (usually as 25% with reference to different jurisdictions AML laws and regulations, or 10% as per different financial
institutions compliance and KYC policies)\textsuperscript{17}, which means sanctioned entities had a much lower threshold to consider in order to circumvent the OFAC 50% rule.

Hence, no matter how complex of the ownership structure of the asset holding entities, the whole ownership information and related percentage of ownership is made transparent to financial institutions.

Thus, other than using just complex structures and multiple layers to conceal the beneficial ownership information, criminals or sanctioned entities would also use shell companies, shelf companies, and front companies to circumvent sanctions regulations. Shell companies, from 2014 FATF’s \textit{Guidance on Transparency and Beneficial Ownership},\textsuperscript{18} are defined as “Companies that are incorporated but which have no significant operations or related assets.” Shelf companies, on the other hand, had been created several years prior and allow new owners to secure company structures within a short period of time, given the time-sensitive need for business dealings. Front companies differ from shell and shelf companies by being a “fully functioning company, with assets, income and expenses as legitimate company with business operations.”

Sanctioned entities or countries can easily create shell companies or purchase readily available shelf companies with assistance from trust and company services providers (TCSP).\textsuperscript{19} Although this sanctions

\textsuperscript{17} For example, both Hong Kong and Singapore’s AML regulations determine 25% or more shareholders to be ultimate beneficial owners (while Hong Kong had reduced the threshold from 10% to 25% in year 2018):
https://www.accountingsolutionssingapore.com/changes-to-companies-act/

\textsuperscript{18} See http://218.189.123.38/videoplayer/Guidance-transparency-beneficial-ownership.pdf?ich_u_r_i=e3bb390d660903323232e8fad168ab5a24&ich_s_t_a_r_t=0&ich_e_n_d=0&ich_k_e_y=2045028919751563512414&ich_t_y_p_e=1&ich_d_i_s_k_i_d=8&ich_s_e_q=735634639&ich_u_n_i_t=1

\textsuperscript{19} From various searches, trust and company service providers have various shelf companies ready to be sold to their customers. As one of their major business revenue streams, trust and company service providers could also even guarantee or provide bank accounts associated with these shelf companies as per below:
circumvention technique has been identified by the United Nations in investigations,¹⁰ this technique is still one of the major techniques used by sanctioned entities or countries due to the following reasons:

A. Shell and shelf companies controlled by sanctioned entities are hard to detect and identify as their incorporation is no different from other companies formed for other purposes. It will be even more hard to identify for corporates incorporated in offshore jurisdictions, as the registered address is usually located at the same address of the company service provider. There is a limited source of information to identify 1) the actual physical address and 2) the actual business activity of corporates, in order to determine whether the corporate is a shell, shelf company, or a normal business.

B. The other reason lies in the fact that because several jurisdictions lack AML/CTF regulations and guidance on trust and company service providers,²¹ there are vulnerabilities in circumventing both

https://www.ck-tax.com/readymade (asking for HKD 50,000 per each company with readily available bank accounts)
http://www.hkgfssl.com/klyhhk.html
http://www.asiabs.com/chineset/chineset_company_formation_hong_kong_service_fee.htm
http://www.eabhk.com/eabhk-1.html
https://www.easyaccounthk.com/cr/

From media news during the Panama Papers leakage, it is known that accounting firms were asking for HKD 5,000 to assist clients to open new companies, and as nominee directors/shareholders:
https://hk.nextmgz.com/article/2_391980_0

²⁰ North Korean banks and firms, meanwhile, have maintained access to international financial markets through a vast network of Chinese-based front companies, enabling Pyongyang to evade sanctions, as per a confidential UN report in 2017:

Global Communications is a defence company that sells battlefield radio equipment and accessories. Its website claims it is based in Malaysia. However, in 2017, a UN report, submitted to the United Nations Security Council, claimed that Global Communications was a front company for the government of North Korea in order to sell military equipment in violation of UN sanctions:
https://en.wikipedia.org/wiki/Glocom_(defence_company)

²¹ FATF’s Mutual Evaluation Report on Hong Kong (2019) highlights that previously Hong Kong’s TCSPs were not being regulated under the AML regulations until late 2018. Moreover, there were “no specific provision that requires TCSPs to identify and assess the risks specifically in relation to the
money laundering and sanctions regulations. First, since shell or shelf companies have no physical presence, the address will be the same with TCSP. Second, nominee directors and management would be using the ones provided by the TCSP, and actual ownership will be not be updated nor will be concealed for financial institutions up until the point when there would be a triggering event for an ad hoc review or during a periodic review (use of nominees is also one of the sanctions circumvention technique to be discussed.).

C. Front companies, on the other side, could facilitate the normal and long-term operations or movement of funds by sanctioned entities. Better than shelf and shell companies, front companies could even conceal the source, the country where the funds are generated and beneficial ownership in a more general way. Front companies have normal and legitimate business operations, which could disguise the source of funds, which were derived from sanctioned entities or countries, as either increase in business scope, revenue, or new countries of operations, and

development of new products and new business practices, and the use of new or developing technologies prior to launch or use of such products, practices, and services." Under FATF’s recommendation 22 and 28, Hong Kong was being rated as partially compliant in mutual evaluation 2019: https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-Hong-Kong-China-2019.pdf

FATF’s Mutual Evaluation Report on China (2019) highlighted that there were no AML laws coverage on company service providers, although before the mutual evaluation on China that Chinese authorities issued Notice of the General Office of the People’s Bank of China on Strengthening the Anti-Money Laundering Supervision Work on Designated Non-Financial Businesses and Professions, 2018. However, this notice is not being included in the AML regime and laws in China; hence, China was being rated noncompliant for FATF’s recommendations 22, 23, 28:

For other tax havens in South Pacific countries like Solomon Islands, under their Mutual Evaluation Report for FATF’s recommendations 28: It is noted that there was no supervision policy from regulators on the frequency and intensity of the AML/CFT supervision informed by ML/TF risks, the nature of the various TCSPs, and size of the various reporting TCSPs. Also, there were no requirements that compel the competent authorities in Solomon Islands to take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest or holding a management function in a TCSP:
prevent the funds from being identified by the financial institution’s transaction monitoring systems (which is better than shell or shelf companies as these companies with no business operations before).

D. The last reason lies in relation to financial institutions and intelligence agencies. Given the ease of initiating new shell companies, or purchasing shelf companies from TCSP, the cost to sanctioned entities or countries is limited compared to the huge cost to financial institutions and the intelligence investigation unit (U.N. Panel) for identifying the shell or shelf companies controlled by sanctioned countries or entities. Furthermore, OFAC’s *A Framework for OFAC Compliance Commitments* highlighted that another root cause of a sanctions compliance program’s failure is related to sanctions screening software or results filtering. Financial institutions may fail to update the sanctions screening software to incorporate changes with reference to the latest SDN or SSI list, entities under 50% OFAC rule.

For financial institutions (and even worse for smaller banks or payment companies), there would be no additional cost or manpower to further identify entities that should be blocked under different sanctions regimes with which financial institutions must comply. Hence, financial institutions could only passively rely on intelligence agencies to update their sanctioned entities database for screening and maintain daily operations. The effectiveness of sanctions screening software is being reduced (or even financial institutions, law enforcement agencies, immigration units could not able to identify sanctioned entities with no further information provided from intelligence agencies). For sanctioned entities or countries, it would be good news as financial institutions could

---

22 From financial institutions’ general policies, there were CDD/KYC reviews to be performed on reactivated dormant accounts; there were also transactions monitoring scenarios on account activity of inactive customers. Using front companies with normal business operations could prevent detection from monitoring scenario and performance on KYC/CDD review from financial institutions.

23 Refer to Case Study 2: Fight for the Second Life - A True Story of a Former Sanctioned Individual.
not able to identify their shell, shelf, or front companies during normal payment screenings using their sanctions screening software. Sanctioned entities or countries could just buy another shell, shelf, or front company from the TCSP if some of them have been identified or if their accounts have been closed by the financial institution.

B. Concealment of Payment Information

In reference to OFAC’s *A Framework for OFAC Compliance Commitments*, another root cause of failure of a sanctions compliance program is related to processing payments or commercial transactions through financial institutions involving sanctioned countries or countries. Although the transactions may not physically involve the United States while the payment is being routed in United States for clearing purpose (payment in USD), the payments would be cross-border remittances.

As mentioned, financial institutions or entities process payments, or commercial transactions would be subjected to heavy fines or other penalties from law enforcement agencies. However, sanctioned entities, other than getting assistance from financial institutions (which most of settlement cases for financial institutions indicated), could also use their own methods to make sure payments could be processed undetected by sanctions screening software and transaction monitoring systems.

One of the methods to conceal payment information is wire stripping. Wire stripping is the deliberate act of changing or removing material information from wire payments or instructions, thereby making it difficult to identify and restrict payments to and from sanctioned entities or countries.

24 Ibid.
25 Refer to the settlement agreement between OFAC and Standard Chartered Bank in 2019L
https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190409.aspx
A simple but useful form of stripping, in payment processing, is the inclusion or the use of symbols or a meaningless string instead of the actual payment information (involving sanctioned countries or entities) within the remittance message. An example is:

Translation: “Please use the term ‘GLO FEB 20 F’ as the information in the remittance information. Please DO NOT use terms ‘North Korea,’ ‘DPRK,’ 'Democratic People’s Republic of Korea’ in the remittance information.”

This method could render the sanctions screening software totally useless as there is no clue to identify that the above payment is in relation to DPRK.

For more complex and large-scale wire stripping, so-called “assistance” is required from financial institutions. Regarding recent enforcement actions on financial institutions, it is known that financial institutions have told their sanctioned clients from sanctioned countries to conceal their involvement for sanctioned-related payments and to evade sanctions screening software designed to prevent sanctioned entities from gaining access to the U.S. banking system. 27 Besides changing sanctions screening software (which may leave change logs, or trace changes to identify such actions), financial institutions may also alter the SWIFT remittance message directly, including removing information which could be linked to sanctioned entities or regimes in the MT103 payment message and replace with innocuous information, such as using the bank name itself as one of the transaction counterparts. This could

---

also make sanctions screening software useless as there would be no other red flags or hits being raised from the altered remittance information.\textsuperscript{28}

Another method to alter payment information is to use non-transparency cover payments; again, this method requires “assistance” from financial institutions. The cover payment method involves splitting an incoming MT203 SWIFT message into two different message streams—one MT103 message that includes all transactions details to be sent to the beneficiary bank directly, and the second message, as a MT202 message that has no information on the transaction to be sent to correspondent clearing bank. In this way, there would be no details indicating said transaction would be a sanctioned-related transaction for clearing banks (as there are no transaction details at all).

Again, such “assistances” provided from a financial institution is also one of the root causes of failure of sanctions programs as utilizing non-standardized payment or commercial practices to complete transactions.\textsuperscript{29}

If there were no “assistance” to provided from financial institutions, sanctioned entities or sanctioned countries, in combination of using shell, shelf, and front companies, indirect transfer or payment via third parties would be an alternative way to conceal actual payment information. By breaking down direct payments into multiple payments involving multiple companies, it could be easier to break down the information for sanctions-related payments into several fragments within various payments to facilitate funds transfers. As the information is being fragmented, it could be more difficult for financial institutions to rely on sanctions screening software to detect such payments.\textsuperscript{30} Financial institutions could only


\textsuperscript{29} Several reasons underlying would be: 1) There is not much compliance special attention paid to non-traditional, non-standardized payment methods, including lack of resources for sanctions screening software to handle the same standard for non-standardized payment methods (or simply, the cost effectiveness is low); and 2) it requires some “assistance” from financial institutions that have other methods, including ethics training and whistle-blowing hotline as mitigation measures.

\textsuperscript{30} Depending on sanctions screening software settings and algorithms, partial sanctions-related information may not be detected by the software, as per comparison below.
be able to trace the direct counterpart for the source and destination of funds.\textsuperscript{31} For law enforcement agencies or investigative agencies, it could be more difficult to trace the fund transfers, sources, and destinations of funds with involvement of other unrelated third parties, same name transfers within different financial institutions.

Several entities have been penalized by law enforcement agencies due to wire stripping, or usage of third-parties shell, shelf, and front companies to deal with sanctioned clients (but there were several other reasons for being discovered—for example, being too stupid).\textsuperscript{32} The latter technique, ever evolving and effective, in combination with concealment of beneficial ownerships, is harder to trace by financial institutions and investigative and intelligence agencies (the effectiveness is decreased while cost is increased, good news for sanctioned entities and countries).

C. Cryptocurrency

The cryptocurrency era began in 2008 when an individual named Satoshi Nakamoto published a paper entitled \textit{Bitcoin: A Peer-To-Peer Electronic Cash System}\textsuperscript{33}, in which Nakamoto described a peer-to-peer version of sending cash from one entity to another entity directly without using a financial institution as an intermediary, which further realized the concept of the cryptocurrency named Bitcoin as one of the blockchain applications. Bitcoin, created by

\textsuperscript{31} For financial institutions, which one would be a more suspicious transaction counterpart: 1) same-name transfers to other financial institutions, or 2) an unrelated third-party counterpart under the risk-based investigation approach?

\textsuperscript{32} Refer to ZTE’s case and BIS documents on how BIS further identified ZTE Corporation’s dealing with its Iranian clients in 2018:
https://www.acams.org/aml-resources/acams-europe-blog/sanctions-and-stripping-a-continuing-risk/

Refer to the report from C4ADS regarding North Korea Government’s sanctions circumventions on importing high-end luxury goods by using indirect trades, Russian front companies controlled by Pyongyang Government:
https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d307a43bf42140001877def/1563458128965/Lux+%26+Loaded.pdf

\textsuperscript{33} “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto, 2008:
https://bitcoin.org/bitcoin.pdf
Nakamoto, sought to solve the accounting problem of “double spending” by using transactions linked to previous transactions as a public open ledger, which is the prototype of current blockchain technology. Since the initial transaction on 12 January 2009, Bitcoin was publicly implemented on 22 May 2010\(^\text{34}\) with an exponential increase in terms of user base and popularity.

Cryptocurrency is a digital asset designed to work as a medium of exchange. Cryptocurrencies use strong cryptography to secure financial transactions, control the creation of additional units (blocks/coins), and verify transfers of digital assets. Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems. The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database. Since the release of Bitcoin, over 6,000 altercoins (alternative variants of Bitcoin), other cryptocurrencies, or forms of tokens as digital assets have been created.\(^\text{35}\)

Cryptocurrencies, in several ways, have advantages compared to the use of fiat currencies. Cryptocurrencies are actually pseudonymous. Cryptocurrency wallets are only physically tied to the IP address of the wallet user, where no personal information related to the wallet user can be retrieved from the public ledger information. Thus, sanctioned countries or entities would be able to not disclose (even not conceal) the beneficial owner’s information, which is better than the use of traditional financial institutions services. The IP address of the wallet user could also be disguised by using a VPN network.

\(^{34}\) The first ever transaction of Bitcoin happened on 12 January 2009; a transaction of 50 BTC from Satoshi Nakamoto to computer scientist Harold Thomas Finney II at block 170: https://www.blockchain.com/btc/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

The first public transaction for Bitcoin happened on 22 May 2010 (which is also called as Bitcoin Pizza Day); a programmer named Laszlo Hanyecz bought Papa John’s pizza for 10,000 BTC: https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

\(^{35}\) For the entire list of crypto-related tokens, see: https://coinmarketcap.com/all/views/all/
Also, using cryptocurrencies would involve fewer intermediaries. A single cross-border payment could involve at least three different financial institutions, which include the ordering institution, clearing (correspondent) institution, and the beneficiary institution, before reaching the ultimate beneficiary’s account. This simply means that there could be three sets of different sanctions screening software and databases to pass through in order to effect the transaction. Using cryptocurrencies as fund transfers directly from sender to ultimate beneficiary would also not be subject to the sanctions screening software’s green light (as there would not be one in the public ledger or in the blockchain network, as the network is a decentralized network). Cryptocurrency transactions could also not require the payment information, transaction rationale to reference the transactions, or approval by the intermediaries (actually there are no intermediaries available in cryptocurrency transactions), and the miners actually receive fees as part of the blockchain network to handle the transaction. Thus, it would be easy to pass funds through using cryptocurrencies.

Furthermore, similar to use of TCSP for creating shell, shelf, or front companies for sanctioned entities or countries, cryptocurrency wallets could be created very easily and at low cost (or even no cost). Moreover, there are even fewer regulations in using cryptocurrencies and dealing with them.36 On a macro

---

36 Singapore enacted the Payment Services Act 2019 that regulates payment service providers and payment systems, including cryptocurrency-based payments: https://www.pymnts.com/cryptocurrency/2020/singapores-payment-services-act-to-regulate-crypto-firms/

The Hong Kong Monetary Authority (HKMA) and Securities and Futures Commission (SFC) recognized cryptocurrency as a virtual commodity. Initial Coin Offerings (ICOs) as security token offerings (STO) were subject to existing Hong Kong’s regulations. Moreover, Hong Kong is currently engaging sandbox programs for cryptocurrency exchange platforms and proposed several licensing requirements: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/hong-kong

Although China described blockchain technology as one strategic frontier technology that required the country to develop methodologies and practical applications, the government places heavy restrictions on cryptocurrency, which shall not be being treated as currency in paying for products or services. Furthermore, financial institutions are also prohibited from offering cryptocurrency-related services, banning all ICO activities and cryptocurrency exchange platforms: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/china
level, regional or supranational units have no advisories or guidelines on handling sanctions or money laundering related transactions on cryptocurrencies.\textsuperscript{37} The slow-paced movements of regional advisory and regulatory bodies make available time and space for sanctioned entities and countries to move funds easily. Similarly, when cryptocurrency wallets related to sanctioned entities or countries are identified by investigative intelligence agencies, the same approach could be applied to the replacement of shell companies for cryptocurrency wallets that is in a way faster and more convenient. However, there is still a need to disguise the remaining digital assets before transferring to the “new” wallet, as the public ledger could trace fund transfers and link to identified wallets.

Although OFAC’s sanctions regimes include cryptocurrencies, cryptocurrency wallets and addresses within their sanctions regimes, as part of the sanctioned entities and assets,\textsuperscript{38} related transactions are required to be blocked by financial institutions and taken action against entities using cryptocurrencies for cyber-related crimes and sanctions-related transactions.\textsuperscript{38} As per OFAC’s FAQs,\textsuperscript{39} the agency would only add cryptocurrencies’ addresses on their SDN list (where these addresses could not be searchable by using OFAC’s interactive search tool) and would require filing from financial institutions; the effectiveness of identification of sanctions-related payments with using cryptocurrencies has room for improvement.


In Taiwan, the government intends to launch STO regulations: https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/taiwan

\textsuperscript{37} However, globally there were several guidance papers/consultations being released by countries on how to regulate digital assets. FATF published a \textit{Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers} in accordance with FATF’s recommendations on handling virtual assets due to the increasing use of virtual assets for money laundering and terrorist financing in June 2019: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html


\textsuperscript{39} See https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx
However, there are also some disadvantages to using cryptocurrencies for sanctioned entities or countries. First, digital assets are very volatile. The prices of cryptocurrencies are much more volatile than typical securities listed on a normal stock exchange (no matter whether publicly known cryptocurrencies such as Bitcoin, Etherium, or low-profile tokens with low transaction volumes). Hence, the value of cryptocurrencies per unit of fiat currencies has high fluctuation compared to normal foreign exchanges within different fiat currencies; this creates a high operational risk for sanctioned entities and countries to make normal payments in terms of cryptocurrencies. (For stable coins, the stance of fluctuation still exists but less in terms of how the coins’ value is fluctuating.)

Another difficulty for using cryptocurrencies is in relation to the process of exchanging with fiat currencies, as the beginning and the end in the process chain. This process involves and usually needs to deal with cryptocurrency exchanges as a middleman to handle cryptocurrencies—fiat currencies transactions. For cryptocurrency exchanges, there exists a certain level of AML and KYC requirements for their customers (identification verification, source of funds of customers, disclosure of transaction rationale); however, this will damage the anonymous nature of cryptocurrency transactions. Furthermore, currently there is no standardization of AML requirements for cryptocurrencies exchanges. Their level of AML and KYC depends on the business nature and management nature of exchanges. (However, in the cryptocurrencies industries, the industry players tend to be regulated in order to be fully recognized publically, which means the level of AML and KYC requirements will be increased, and gaps with traditional financial institutions will be reduced.)

regarding cryptocurrency transactions (due to their irreplaceable, permanent blockchain nature), transaction information (including wallet address, amount, time of transaction, additional input by users of the transactions) could be

---

40 Ibid. (37)
41 See https://www.elliptic.co/our-thinking/bitcoin-money-laundering
42 See https://qz.com/1761343/bitcoin-money-laundering-is-a-classically-stupid-crime/
identified or derived anytime by investigative agencies. Similar to money laundering, it is necessary to leave a minimal trace for investigative intelligence agencies to identify sanctions-violation issues (as investigative agencies start to work with companies with developing cryptocurrency-transaction monitoring systems).43

Thus, although the payment time for cryptocurrencies is much faster than for traditional fiat currencies, there are no sanctions screening software issues to be considered. The remaining fundamental critical issue or concern in using cryptocurrencies for sanctioned countries and entities, including dealing with cryptocurrency exchanges, is the permanent feature on the public blockchain ledger. At this time, using cryptocurrencies for sanctions circumvention is just a temporary solution in accordance with the unrestricted crypto-regulatory environment.

Case Studies

A. Nation’s Mission – Import Crude Oil from Iran

This is the case of how strategic cooperation between nations takes a higher priority for maintaining sanctions compliance for financial institutions, especially state-owned financial institutions. This case comes from Chinese oil giants and other companies engaged with Iranian clients to do business under the strategic country relationship between Iran and China under Chinese’s Belt and Road Initiative.

Chinese state-owned oil companies, Chinese National Offshore Oil Corporation, Chinese National Petroleum Corporation, and China Petroleum and Chemical Corporation, together with other Chinese-based oil companies, engaged with Iran oil companies like National Iranian Oil Company for an oil or natural gas production project in various oilfields in Iran.

43 For example, a Fintech start-up called Chainanalysis engages in development of transactions monitoring systems in cryptocurrency aspects for governments and financial institutions: https://www.chainalysis.com/
Chinese companies engage the whole Engineering, Procurement, and Construction (EPC) process in these oil projects with Iranian companies, where other companies could engage in overseas operations by simply following the top three Chinese oil giants (which is also one of the major objectives of Belt and Road Initiative). Hence, during operation, oil companies need to cooperate with financial institutions for enabling performance bonds/contracts, trade financing of crude oil, and shipments as the financing part of the process.

In the past days, there were no tight sanctions regimes against Iran, and there were OFAC exceptions on exporting crude oil from Iran to China, the Chinese-side import from Iran in cooperation with Chinese state-owned financial institutions. As both the oil importers and financial institutions were both major state-owned companies, the companies were having a good relationship, where financial institutions were willing to operate with their client’s Iran business.

However, around 2011–2012, there were tightened sanctions regimes from the United States and EU on Iran’s oil industries. However, the Beijing government, despite sanctions regimes, still imports oil from Iran as there is a severe energy shortage in China that requires energy fuel to support Chinese economic development. Thus, this is a strategic nations’ mission to successfully import oil from Iran.

The Chinese side had picked up Bank of Kunlun, under the Chinese oil giant CNPC to facilitate direct payments and trade with Iranian companies. However, the OFAC sanctioned Bank of Kunlun in 2012. Meanwhile, OFAC also prohibits U.S. banks from opening a correspondent-banking relationship with Iranian banks.\(^{44}\)

---

\(^{44}\) See https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_iran.aspx
Bank of Kunlun, after that, still allows payments and provision of trade services in an informal way,\(^{45}\) as the trade between China and Iran reached USD 12 billion annually, and China buys one-third of Iranian crude oil.\(^{46}\) International banking for Iranian companies relies heavily on Bank of Kunlun. Meanwhile, as per disclosure from Bank of Kunlun, the bank may cease Iran-related payments beginning April 2020 to comply with U.S. sanctions regimes. However, non-sanctioned Iran payments are business as usual.\(^{47}\)

In such case, even for sanctioned entities, there is still some space to incorporate financial transactions with using other currencies via the Bank of Kunlun or other international banks in order to evade U.S. sanctions regimes.\(^{48}\)

**B. Fight for the Second Life – A True Story of a Former Sanctioned Individual**

This is a real-life story of a former OFAC-, EU-, and U.N.-sanctioned individual, Mr. Y. As Mr. Y was financing and providing weapons to Charles Taylor for Charles Taylor’s activities in Liberia during the Liberian civil war in exchange for competitive advantages for Mr. Y’s family forestry business.

The story of Mr. Y could be traced back two decades ago. Mr. Y is reportedly a Chinese-Indonesian who was born in Malaysia and has Singaporean citizenship. Mr. Y is the eldest son of a Chinese-Indonesian “Timber King.” Mr. Y worked under his father’s organization since 2000. In a disclosure report from the U.N., Mr. Y reportedly worked in Liberia since 2003 for his family’s timber

---

\(^{45}\) See https://www.bourseandbazaar.com/articles/2019/1/2/policy-change-at-chinas-bank-of-kunlun-cuts-sanctions-lifeline-for-iranian-industry


\(^{46}\) See https://www.atlanticcouncil.org/blogs/iransource/china-iran-s-lifeline-to-overcome-oil-sanctions/

\(^{47}\) Ibid.

\(^{48}\) Similarly, Macau-based Delta Financial Group reportedly has been dealing with funds from North Korea since the 1970s. On 15 September 2005, the United States Department of the Treasury designated the Delta Financial Group as a "primary money laundering concern" under Section 311 of the USA PATRIOT Act. It was alleged that the Delta Financial Group represents an unacceptable risk of money laundering and other financial crimes as it has been a willing pawn for the North Korean government to engage in corrupt financial activities through Macau:

business together with his relatives. It is known from U.N. report that Mr. Y is actively financing Charles Taylor.

Mr. Y was listed on the EU, U.N., and OFAC sanctions list during the time of 2003 to 2012 under his former name due to his close relationship with Charles Taylor. However, during this time, Mr. Y had already changed his legal name (both Chinese and English), which had not been identified by any law enforcement agencies, financial institutions, or intelligence unit.

Mr. Y was approved to become a Hong Kong resident through Hong Kong’s Capital Investment Entrant Scheme in 2012, and became a permanent resident in 2019. However, the sanctions program against Mr. Y was only halted in November 2015 (OFAC, U.N.) and December 2015 (Hong Kong).

Mr. Y first engaged Bank A for a banking relationship when he was approved to come to Hong Kong in 2012. He later closed the accounts with Bank A. Mr. Y came to Bank B to engage a banking relationship on 17 November 2015 (the day right after OFAC and U.N.’s termination on sanctions of Mr. Y, or more technically, less than 12 hours after). However, there was no indication of previous sanctions identified for Mr. Y via the internal AML screening system of Bank B during the account opening.

The case of Mr. Y was referred to the compliance department of Bank B in May 2019 through Bank B’s internal suspicious transactions monitoring system. Mr Y’s transactions were first reported to the local financial intelligence unit on July 2019 for some doubtful incoming funds during the sales process of a shrimp aqua farm in Indonesia owned by Mr. Y and his family. However, the first compliance officer of Bank B did not identify related sanctions information on Mr. Y via open source information at the initial time of filing.

During a triggering event that resulted in an account review for Mr. Y, the middle office operations officer discovered potential adverse information regarding Mr. Y using his current legal name in Hong Kong, and then escalated the case back to the compliance team of Bank B. The second compliance officer of Bank B
later confirmed the adverse information as a true hit against Mr. Y. The second compliance officer of Bank B later filed another suspicious transaction report on Mr. Y (and all related accounts) to the local financial intelligence unit. However, due to a serious business concern, Bank B maintains the entire business relationship with Mr. Y’s family group, despite the fact that Mr. Y’s source of wealth came from activities related to Charles Taylor during the sanctioned period.

In this case, Mr. Y changed his legal name (both Chinese, English and Indonesian), keeps a low public profile, just revealing partial source of wealth information, and avoids revealing previous information from a long time ago. Using a bank without serious AML and compliance requirements, Mr. Y could officially begin his second life in Hong Kong.

C. Business as Usual – Case of Firms in Crimea

This is a case regarding how western companies could still engage in business in the Crimean region of Ukraine under the sanctions regimes applied to the region that resulted from Russian military intervention in Ukraine and the annexation of Crimea by Russia since 2014.

One example is related to the construction of Kerch Bridge, which connected Crimea and the Russian mainland. It is reported that two Dutch companies, namely Dematic Equipment and Bijlard Hydrauliek, were engaged with the Russian government to provide machines, parts, and related services for the construction of this bridge. Dematic Equipment first shipped the parts prohibited to Russia in 2016; the parts were being assembled in Russia and then shipped to Crimea for construction later. The company acknowledged the parts were being assembled and shipped for construction of the bridge. Meanwhile, Bijlard Hydrauliek established a front intermediate company in the Netherlands to

---

49 Ibid. (4)
50 See https://en.wikipedia.org/wiki/Crimean_Bridge
handle this transaction. Both companies denied that the activities violated the sanctions regime.

In this case, western companies tried to evade sanctions regime through the use of front companies, once again, and isolation model, which uses an intermediary process step to obfuscate relevant investigations and due diligence process by financial institutions.

Another example is related to shipping companies when western restrictions were imposed on shipping activities in the Crimean region, where shipping activities were reduced reportedly 50% in 2014 when sanctions were imposed. However, the shimming activities were back to normal in 2015.

Shipping companies use manipulative techniques to evade sanctions when shipping companies use fictitious names, change operating companies frequently, and register these vessels with convenience flags in the Crimean region (e.g., Panama, Russian, Togo) where the vessels are bound with the rules of country of registration. Moreover, vessels would also turn off radar to avoid trace of routing, which relevant sanctions circumventions methodologies were being highlighted from OFAC’s “Sanctions Advisory for the Maritime Industry, Energy and Metals Sectors, and Related Communities”51.

How Can Financial Institutions Face This Evolving Situation?

Financial institutions, as mentioned, were only able to face the ever-changing sanctions regulatory era passively as sanctions are currently being treated as a tool for countries to force other countries or entities to change their unwanted behaviour. Being involved in political wrestling between different countries, financial institutions in order to prevent their normal business from being disrupted or heavily fined had no other choice but to follow major sanctions regimes, as a foundation, and paid huge

51 https://www.treasury.gov/resource-center/sanctions/Programs/Documents/05142020_global_advisory_v1.pdf
operations costs to maintain the sanctions regulations, which led to the formation of sanctions compliance programs.

An internal audit function, being the third line of defence, is responsible for providing assurance to the financial institutions’ board of directors and senior management with regards to how effectively the financial institution assesses and manages its sanctions-violations risks, which will also include providing assurances on the effectiveness on the first and second lines of defences. The assurance assessment encompasses all elements of a financial institution’s own risk management framework and organizational objectives.

Different from first and second lines of defences, the internal audit function positions itself as an advisor on how to coordinate assurance, to effectively measure and improve existing process, and to assist management in the implementation of recommended improvements. The internal audit function, as the third line of defence in a financial institution, is one cornerstone for the corporate governance. Thus, the internal audit function’s role and objective to handle sanctions compliance risk would be assurances on front line (as first line of defence) and compliance’s (second line of defence) effectiveness and implementation of sanctions compliance program to ensure a internal sanctions compliance program could adhere with supranational and countries sanctions regime.

OFAC’s *A Framework for OFAC Compliance Commitments* highlights and encourages financial institutions to employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating the sanctions compliance program. Meanwhile, the sanctions compliance program should maintain five essential components as (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing, and (5) training. The audit function and objective includes providing assurances by identifying a financial institution’s sanctions compliance program’s weaknesses and deficiencies, and ensuring the implementation of a financial institution’s responsibility to enhance its program, including all program-

---

52 See https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/
53 Ibid.
related software, systems, and other technologies, and to recommend the remediation of any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating sanction compliance program elements to account for a changing risk assessment or sanctions environment. There is a wide scope for internal audit function to maintain the effectiveness of the existing sanctions compliance programs.

However, the first thing for auditors, other than checking on policy and procedures, is to understand the nature of sanctions regimes and how these regimes are related to financial institutions. There is no warning\(^5\) from authorities before issuing penalties on financial institutions. Auditors also need to be aware if the additional risk being posed to financial institutions for changes in sanctions regimes within this international conflict era. Auditors should also consider the management and financial crime compliance team’s responses on updates of sanctions compliance issues. Are there any existing exposures to sanctioned countries and entities? What mitigation measures will be done if there have been potential sanctions violations issues? Financial institutions could choose to: 1) do business as usual, continuing to do transactions with possible sanctions violations;\(^6\) 2) approach transactions one by one and analyse the sanctions regime on a case-by-case basis; or 3) just simply ban all transactions.

After considering the normal business strategies and objectives, auditors could identify, develop, and test internal controls within financial institutions to mitigate the inherent risks and exposures. Furthermore, as there are more evolving circumvention techniques, auditors should pay more attention to testing relevant circumvention controls and weakness of sanctions compliance programs highlighted by authorities.

\(^5\) See https://www.lexology.com/library/detail.aspx?g=cb40397f-66f9-4ce1-8e37-353e11d51f16

\(^6\) Refer to the case of Kunlun Bank, which reopened processing of Iran-related payments in 2018, but was stopped again in January 2019. However, facilitation of oil shipments from Iran to China was conducted again in mid-2019 and created huge chaos for China-United States-Hong Kong’s relationship (further refer to Case Studies 1: Nation’s Mission):
https://www.cnbc.com/2019/05/30/a-single-oil-tanker-could-become-a-factor-in-both-the-china-trade-war-and-iran-tensions.html
As mentioned in OFAC’s *A Framework for OFAC Compliance Commitments*, other than the common root causes in relation to AML, KYC, and CIP functions, specific sanctions related to failure lie in sanctions screening software’s filtering fault and inconsistent implementation of sanctions compliance programs.

In handling the test of controls of sanctions screening software, auditors should access the appropriateness of financial institutions’ sanctions screening process with regards to the organization’s business nature, scale, complexity, client base and jurisdictions, and products and services being provided. Auditors also need to assess whether the sanctions screening process complies with normal policies and procedures.

Other than assessing the sanctions screening process, auditors are also required to have assessments on the sanctions screening databases, including the latest lists provided from intelligence agencies or authorities local sanctions list, and watch list entities. Auditors are to assess if the financial compliance team had entered all relevant and required lists into the sanctions database, the timeliness of updating sanctions lists entities and information into the database (including automated and manual updates), as well as the process of updating and approval of updating such information into the sanctions screening database.

Meanwhile, other than keeping the database current with black-listed entities, there is also the “good guy” (white list) in the sanctions database which should also be managed for operational efficiency, false hits reductions, and as other exclusion with reference to business objectives to the sanctions screening software. Auditors should assess controls to maintain the good guy list and ensure: 1) The good guy list does not contain sanctioned entities and countries; and 2) the periodic review of good guy list. As mentioned, there is the use of alternative transaction data to make the sanctions screening software useless. In this regard, auditors need to assess the process and transmission of SWIFT messages within different systems in financial institutions and cross financial institutions to ensure complete, timely, and accurate data transfer to maintain the effectiveness of sanctions screening software.

---

56 Ibid.
Another emphasis is related to circumvention controls. The financial institution, in order to be compliant with sanctions regimes (and secondary sanctions), should be able to detect and prevent sanctions circumvention through the use of interdiction rules on sanctions screening software and transaction monitoring systems to flag out potential attempts for: 1) resubmitted rejected payments, and 2) payments with involvement of third parties with no apparent business relationships or no business operations to support the payment. Auditors should also ensure that the financial crime compliance team follows up with the confirmed sanctions circumvention incidents (with report to relevant authorities).\textsuperscript{57}

To achieve the objective, auditors could first understand the interdiction rules being placed in the transaction monitoring system and the sanctions screening software. Meanwhile, auditors are to test relevant alerts and sample cases to identify sanctions circumvention cases and payments. If there have been potential sanctions violations cases and issues, auditors should select and assess whether the financial crime compliance team had taken appropriate follow-up measures (e.g., freeze assets, account closure, report to authorities and local law enforcement agencies).

**Conclusion**

Sanctions are tools of supranational entities and countries as one of the measures used before using armed forces to terminate the sanctioned country’s unwanted behaviours. Counter-sanctions activities, conversely, are methods used to circumvent sanctions.\textsuperscript{58} Financial institutions have been only passively involved in this political wrestling between nations. This will be an endless war of sanctions and sanctions circumventions. Audit functions play an important role in financial institutions, ensuring that financial institutions can continue their business goals and objectives in this endless war of sanctions.

\textsuperscript{57} OFAC non-reporting may also be subject to heavy fines as one of the OFAC sanctions violations.

\textsuperscript{58} Iran formed a joint venture bank in Bahrain Future Bank to facilitate payments; or as Bank of Kunlun case: https://www.washingtonpost.com/world/national-security/billion-dollar-sanctions-busting-scheme-aided-iran-documents-show/2018/04/03/37be988a-3356-11e8-94fa-32d48460b955_story.html
References


Blockchain.com. [Date of first Bitcoin transaction 12 January 2009.] Retrieved from https://www.blockchain.com/btc/block/00000000d1145790a8694403d4063f323d499e655c83426834d4ce2f8dd4a2ee

Blockchain.com. [Information on Laszlo Hanyecz buying Papa John's pizza for 10,000 BTC.] Retrieved from https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d


Current Affairs Group. (2016, 5 March). “Panama storm” Hong Kong accountants received 5,000 to help open offshore companies. One Weekly. Retrieved from https://hk.nextmgz.com/article/2_391980_0


Gharagozlou, L. (2019, 30 May). A single oil tanker could become a factor in both the China trade war and Iran tensions. CNBC. Retrieved from https://www.cnbc.com/2019/05/30/a-single-oil-tanker-could-become-a-factor-in-both-the-china-trade-war-and-iran-tensions.html


Taiwan Ministry of Justice. (2018, 11 July). Counter-Terrorism Financing Act. Retrieved from https://www.mjib.gov.tw/userfiles/files/35-%E6%B4%97%E9%8C%A2%E9%98%B2%E5%88%B6%E8%99%95/%E6%B4%97%E9%8C%A2%E9%98%B2%E5%88%B6%E8%99%95-EN/2.pdf


