The Business Crime Solution

Helping Build Practical Compliance Strategies

December 2023

FINTRAC 2022-23 Annual Report

Cyber-Enabled Fraud

Europol Report: Fraud

Wilful Blindness or Greater Detail

Which Is It?

The latest fines from FINTRAC, targeting two of Canada's major banks, shook the reporting sectors across Canada, not only because of the amount of the penalty but also the focus of the cited deficiencies and who was fined. That said, a comment I read today in an email from a respected AML colleague really sums up the thinking about what happened.

Specifically, she asked, "Are Entities just not following the rules and turning a blind eye, or are the audits getting that difficult?" To me, I think it is both realities!

Not following the rules is clearly evident, as RBC and CIBC, were called for not submitting STRs. In the case of CIBC, FINTRAC's examination found an instance where a Suspicious Transaction Report ought to have been filed. Specifically, this case related to a client who had been arrested and charged with criminal offences. Despite knowing this, CIBC concluded that no Suspicious Transaction Report was required as the observed activity appeared to be normal and in line with the client's profile, despite the presence of the ML/TF indicators and contextual information obtained by the Bank. In my view, CIBC knowingly chose to not submit an STR despite all the signs pointing to possible money laundering taking place.

(Continued on page 4)

The Business Crime Solution

Publisher
About Business Crime Solutions, Inc.

Editorial Director
C. Jason Walker

Subscriber & Privacy Services
EDUCON Marketing & Research Systems

Contributing Experts
Christopher Walker, M.Criminology
EDUCON Marketing & Research Systems
Jennifer Wilson, BA, CAMLI-PA
Julian Arend, MA

Yearly electronic subscriptions (12 issues) to *The Business Crime Solution* are available at $250 + HST/GST where applicable (in Canadian funds).

www.moneylaundering.ca

About Business Crime Solutions, Inc.
PO Box 427
Merrickville, ON
K0G 1N0
Phone: **(613) 283-2862**
FAX: **(613) 283-7775**
E-mail: info@moneylaundering.ca

ISBN: **0-9689436-0-8**

In This Issue:

1 Wilful Blindness or Greater Detail: Which Is It?
2 A Word from the Editors
2 Upcoming Events
3 In the News
4 Case Study: Third Party Money Launderers
5 FINTRAC 2022-2023 Annual Report Highlights
6 FATF: Illicit Financial Flows from Cyber-Enabled Fraud
8 The 2023 Geography of Cryptocurrency Report
10 Europol Report: Fraud
12 Cybercrime Money Laundering Red Flags
13 Beyond Our Borders: Somalia
15 Case Study: Transnational Organized Crime

A Word from the Editors

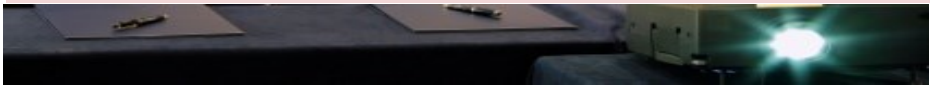
We have dedicated significant space in this month's edition to a number of the reports/research documents that were released in the final months of 2023. FINTRAC's 2022-23 Annual Report as well as releases from the FATF, Europol, FinCEN, and Chainalysis are under the spotlight this month, providing significant insight into current trends and industry red flags.

CAMLI Update:
CAMLI is pleased to announce that six webcast seminars have been scheduled for 2024. Visit our website for the latest on these events and future CAMLI products and services.
www.camli.org

Upcoming Events:

September 16-17, 2024 **Money Laundering in Canada 2024**
Victoria, British Columbia, Canada

more information coming soon



What Is CAMLI?

CAMLI is an education and resource forum for anti-money laundering compliance professionals to further develop and be recognized for their knowledge and skills in the control of risks from money laundering and terrorist financing activity.

The mission of the Canadian Anti-Money Laundering Institute is to provide a broad-based educational forum for anti-money laundering compliance professionals in Canada to further develop and be recognized for their knowledge and skills in the control of risks from money laundering and terrorist financing activity.

CAMLI

www.camli.org

In the News

Money Laundering Operation Leads to Four Arrests

An investigation of Pareto Pharmaceuticals that began in December 2020 led to search warrants being executed in December 2023 at several locations throughout Calgary and in Chestermere, in addition to four vehicles and one location in Vancouver. As a result, a variety of drugs and drug-related products were seized, with a combined street value of approximately $7 million, including: anabolic steroids in both raw and ready to use/sell condition, supplies and equipment for making anabolic steroids, as well as $589,585 in Canadian currency and approximately $500,000 worth of jewelry.

The investigators believe that the owner and operators of Pareto Pharmaceuticals, an anabolic steroid business, acquired millions in sales between 2015 and 2023, and then laundered the money through cryptocurrency and real estate investments. "The production and sale of anabolic steroids is prohibited by the *Controlled Drugs and Substances Act*, and the other bodybuilding products being sold by Pareto Pharmaceuticals are restricted by the *Food and Drugs Act*." Their products were sold in gyms, by online sales reps, and on two websites: paretopharmaceuticals.com and paretopharma.com.

"After analyzing more than 150 bank accounts connected to the Pareto Pharmaceuticals business, investigators determined the money was laundered through the use of multiple bank accounts and securities investments belonging to the accused and their shell companies. Money derived from the Pareto Pharmaceuticals business was also converted into various cryptocurrencies, which was then used for the purchase and sale of real estate."

Three men and one woman are believed to be responsible for the production and illegal sale of anabolic steroids over the course of eight years, resulting in an illegal profit of more than $9 million.

Sources:
https://calgaryherald.com/news/crime/arrests-made-in-9-million-money-laundering-operation

Unexplained Wealth Orders in B.C.

B.C.'s provincial government has begun filing Unexplained Wealth Orders (UWO), a newly created tool under the Civil Forfeiture Act that, when a judge approves, requires people to explain how they acquired funds when they appear to have originated from criminal activity.

Minister of Public Safety and Solicitor General Mike Farnworth would not comment on current cases but made the following statement, "I can confirm that we will continue to forfeit illegally obtained assets, and redirect them to community safety and crime-prevention initiatives, which help repair the damage done by those who think that they can profit from crimes and illegal enterprises in British Columbia."

Lawyer's Trust Account Subject to Unexplained Wealth Order Application

The B.C. Director of Civil Forfeiture seeks the forfeiture of about $3.5 million held in the trust account of Ronald Pelletier, who was disbarred last month by the Law Society of B.C. The claim was filed December 14th for funds held in trust by Pelletier for "Kevin Miller, a man who neither admitted nor denied his role in a US$78 million pump-and-dump fraud scheme, in a settlement agreement with the SEC, in October 2017."

The Unexplained Wealth Order (UWO) would compel Miller to provide details on how the funds were acquired and maintained. The government's claim is that there are reasonable grounds to believe that the money came from the stock market manipulation case that was settled in the US and are proceeds of crime. "Miller filed a claim for the funds last year against the Law Society of B.C., which has frozen the account."

Source:
https://www.cbc.ca/news/canada/british-columbia/bc-canada-first-unexplained-wealth-order-1.7045209

(Front Page - Continued from page 1)
With RBC, FINTRAC noted that it failed to submit sixteen Suspicious Transaction Reports (STRs) where there were reasonable grounds to suspect that transactions were related to the commission or attempted commission of a money laundering (ML) or terrorist activity financing (TF) offence. These STRS included: (a) cases where the Bank was served with production orders on clients and it failed to escalate/refer the files for the purpose of determining whether an STR should be submitted to FINTRAC; observed frauds where STRs were not sent to FINTRAC despite the presence of ML/TF indicators to support the establishment of reasonable grounds to suspect that transactions were related to the commission or attempted commission of an ML offence or a TF offence; and, instances where case investigations were closed citing that no STR was required without adequate review of the client activity against relevant ML/TF indicators.

With both Banks, the findings demonstrated clear failure to follow well-established ML/TF indicators, which provided ample reasonable grounds to suspect that money laundering and/or terrorist financing could have taken place. Wilful blindness beyond a doubt, which definitely warranted a fine being applied.

Now, with respect to the second question, "… are audits getting that difficult?", I would drop the word *difficult* and replace it with *detailed*. If you review the published AMPs over the last half-dozen years, FINTRAC has been elevating the detail to which they are looking at a reporting entity's AML/ATF compliance management program application practices. FINTRAC examinations have moved well beyond checking to see if a reporting entity has its compliance program elements in place. The audit has raised the level of assessment to looking at the detail of those elements. Whether your Policy Manual spells out the detail of what you need to do, followed up by looking at whether the compliance department applies those details. Or, if you will, whether the application details observed are in fact recorded in the procedural component of your Policy Manual.

In the cases of RBC and CIBC, one would expect that their senior management would demand adherence to compliance programs that followed to the letter both the legislative Regulations and FINTRAC Guidance. Especially since very large financial institutions make a very public point that they hold other reporting sectors to those same controls. And yet these AMPs are giving credence to the saying that what is good for one group doesn't always have to apply to another. If RBC and CIBC are so demanding of their entity customers, then they should ensure their own compliance house is in order. Thoughts?

Case Study - Third Party Money Launderers

This investigation focused on a transnational money laundering organization operating in the United States and Mexico through a complex trade-based money laundering (TBML) scheme.

This conspiracy involved couriers picking up drug proceeds in the form of U.S. currency from multiple cities in the U.S. and transporting it by various means to Texas. Once in Texas, the organization laundered the funds through commodities businesses, including perfume sellers, using a sophisticated TBML scheme. The drug proceeds collected in the U.S. were assigned by Mexico-based peso brokers to Mexican import businesses who owed U.S. currency to U.S. export businesses. Part of the proceeds were then delivered to the particular U.S. export businesses as payment for the purchase of goods, while the remainder of the proceeds were transferred through a series of additional transactions to Mexican drug cartels.

Investigative officials from several agencies analyzed a high volume of BSA data to identify the bank accounts of numerous individuals, as well as the money laundering activity occurring in these accounts. In some instances, officials were able to determine that certain BSA forms that should have been reported by the U.S.-based businesses involved had not been filed.

Following a 5-week jury trial, all of the defendants were convicted of various money laundering and conspiracy charges. In total, this organization laundered more than $2.8 million. Approximately $2.5 million was seized during the investigation, and over $870,000 in money judgments were ordered after trial.

Source: https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act

FINTRAC 2022–2023 HIGHLIGHTS ANNUAL REPORT

FINTRAC provided 2,085 disclosures of financial intelligence to its regime partners in support of money laundering and terrorist financing investigations across Canada and around the world.

FINTRAC provided 225 financial intelligence disclosures to foreign FIUs. The top five predicate offences related to case disclosures were:

- 31% Drugs
- 25% Fraud
- 13% Crimes Against Persons
- 12% Human Smuggling/Trafficking
- 11% Tax evasion

DISCLOSURE PACKAGES BY RECIPIENT: 2022–23

Royal Canadian Mounted Police	2,352
Municipal Police	1,050
Provincial Police	670
Canada Border Services Agency	586
Canadian Security Intelligence Service	239
Foreign Financial Intelligence Units	225
Canada Revenue Agency	205
Provincial Securities Regulators	41
Communications Security Establishment	8

FINANCIAL TRANSACTION REPORTS 2022-2023

- Large Cash Transactions: 8,041,942
- Electronic Funds Transfer Reports: 27,315,563
- Suspicious Transaction Reports: 560,858
- Cross-Border Currency Reports/Seizure Reports: 23,699
- Casino Disbursement Reports: 273,785
- Large Virtual Currency Transaction Reports: 94,790

In 2022–23, the Centre presented information on the value of financial intelligence in relation to the investigation of money laundering, terrorist financing, and other types of financial crime at dozens of courses and workshops throughout Canada organized by the Canadian Police College (Internet Child Exploitation Course), the RCMP (Proceeds of Crime, Child Exploitation and Cryptocurrency Investigator Courses), the Ontario Police College (Fraud and Human Trafficking Investigator Courses), Quebec's National Police College Financial Crime Course, the Canadian Association of Chiefs of Police (Human Trafficking Symposium), the Toronto Police Service (Human Trafficking Conference), the Canadian Centre to End Human Trafficking, and the National Coordinating Committee on Organized Crime.

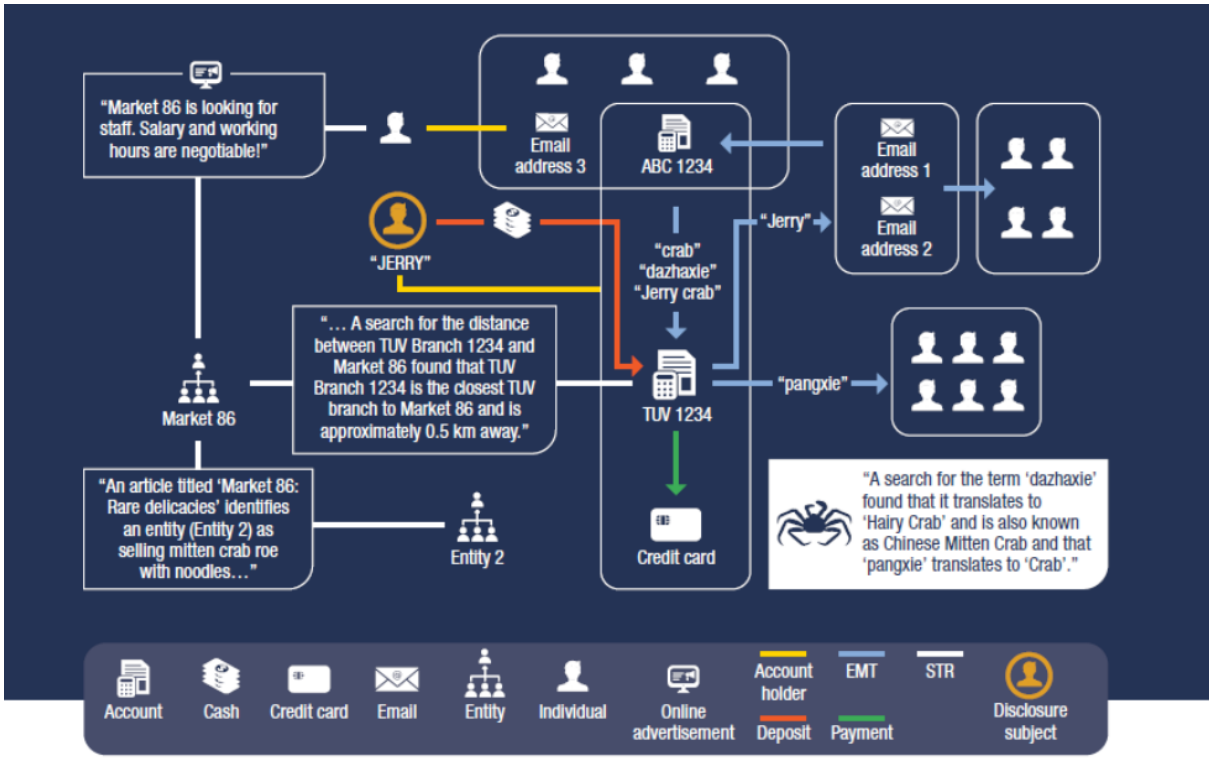
COMPLIANCE EXAMINATIONS 2022-2023

Examinations are one of FINTRAC's primary instrument for assessing the compliance of businesses subject to the Act. FINTRAC uses a risk-based approach to select the businesses that will be examined every year, focusing a significant portion of its examination resources on businesses that report large numbers of transactions or are at a higher risk of being deficient or exploited by money launderers or terrorist financiers. Consistent with its transition from an audit to an assessment approach over the past few years, FINTRAC has undertaken more complex, lengthy and in-depth examinations of larger businesses in higher risk sectors in order to determine how effectively they are fulfilling their compliance obligations.

- 237 compliance examinations were conducted
  - Of the 237 examinations in the past year, the largest number of examination by sector (top three) were: MSBs = 88; Real Estate =71; and Securities Dealers = 38.
- 95% of businesses assessed by FINTRAC did not require enforcement action. This means that these assessments resulted in no further activity or in a follow-up activity instead of enforcement (e.g., data integrity monitoring, a follow-up assessment, an action plan, etc.).

- 81 MSB registrations were revoked
- 6 Notices of violation for non-compliance to businesses
- 10 non-compliance disclosures to law enforcement.

ILLUSTRATING THE FINANCIAL TRAIL (PAGE 39)



Source:
https://fintrac-canafe.canada.ca/publications/ar/2023/ar2023-eng.pdf

FATF: Illicit Financial Flows from Cyber-Enabled Fraud

Cyber-enabled fraud (CEF) is a growing transnational organized crime according to the November 2023 72-page FATF document. This article provides some of the salient features of this detailed report.

CEF criminal syndicates are often well structured into distinct sub-groups with specialized areas of criminal expertise, including money laundering. These sub-groups may also be loosely organized and de-centralized across different jurisdictions, which further complicates efforts to investigate CEF activity. CEF syndicates are also found to be linked to other types of criminality, notably human trafficking and forced labour in CEF call centres. There are also links to proliferation financing, with cybercrime reported as a major source of illicit income generation for the Democratic People's Republic of Korea (DPRK). Illicit cyber activities include the sale of harvested personal information, or the provision of hacking and phishing tools and services, which may be used to by other criminals to commit CEF.

Money laundering groups and professional enablers are involved in the CEF-ML process. The ML network of accounts typically involves money mules but can also include shell companies or legitimate businesses. ML networks also feature different types of financial institutions (FIs), including banks, payment and remittance providers, and virtual asset service providers (VASPs). To further conceal the financial trail of their ill-gotten gains, criminals use a combination of various ML techniques, such as the use of cash, trade-based money laundering (TBML), and unlicensed services.

Aided by digitalization, technology has allowed CEF criminals to develop and increase the scale, scope, and speed of their illicit activities. They use various tools and techniques to deceive victims or prey on their psychological state and emotions to extract as much funds as possible. CEF syndicates are exploiting technological developments to make it easier and faster to launder the proceeds of their crimes. Virtual services, such as remote online account opening, also allow criminals to easily set up foreign accounts and launder proceeds abroad, with financial transactions being executed at near-instantaneous speeds. Criminals are taking advantage of social media and messaging platforms to recruit money mules across borders at scale. Criminals are also quick to exploit vulnerabilities that emerge through new digital financial institutions and products, as well as non-traditional sectors such as e-commerce and social media and streaming platforms.

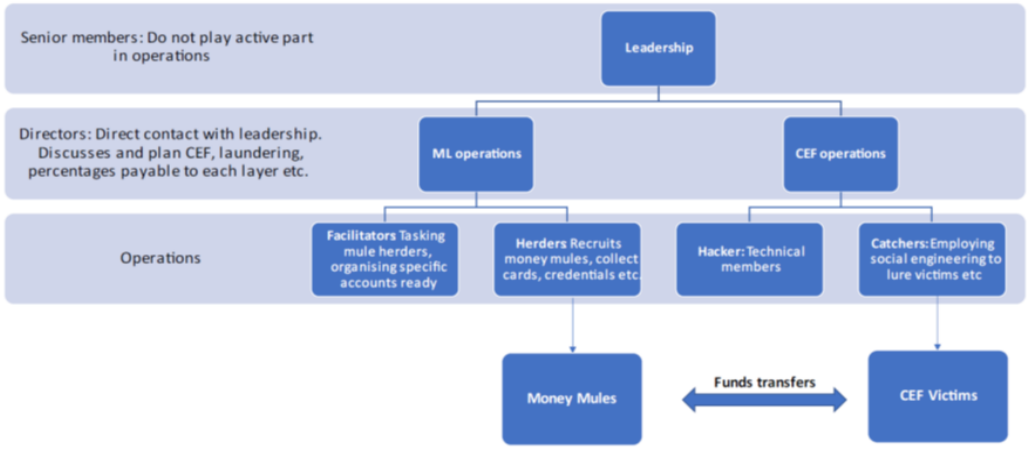
Increased ML Threats:
Americas: CEF has been identified as an increasing or emerging risk. One jurisdiction noted how CEF reports have risen year-on-year, and noted that related ML risk would correspondingly increase. Another reported that investment fraud in virtual assets increased over 180 percent between 2021 and 2022, with criminals taking advantage of the hype and publicity around virtual assets (pg. 10).

The increasingly prevalent use of smartphones, technology (with ever evolving new tools and applications), as well as remote financial transactions, have massively increased the vulnerability of users. Coupled with anonymity-enhancing technology, such as Virtual Private Networks (VPNs) and 'The Onion Router' (also known as TOR - open-source software that allows users to surf the Internet anonymously), this can provide criminals with a cloak of anonymity for their illicit activities. Leveraging technology, criminals can increase the scale, scope, and speed of their criminal activities. Criminals are further observed to be adopting a "Crime-as-a-Service" model, which also significantly lowers the barriers to entry for CEF syndicates, with an increased specialization on different aspects of CEF distributed across different sub-groups.

CEF criminals may rely on one or more of the following elements to successfully deceive victims into making a fraudulent transfer. Different variants of CEF can combine the following elements in different ways.

- Information extraction (e.g., through phishing);
- Social deception or engineering, and preying on vulnerable emotions (e.g., by pretending to be another person or entity and using that as a premise to generate urgency, fear or trust; or by offering false claims to earn money easily); and
- Online medium or platform (that can be either used for communication or for victims to transact on in cases on online trading fraud).

A victim may not fall for just one type of CEF; ultimately, the goal is to induce a funds transfer, and criminals will use a variety of techniques to achieve this. Criminals are creative and may engage or transition to other types of CEF if the initial deception begins to fail. For example, a phishing or social media impersonation fraud victim could be convinced and directed to an investment fraud scheme by the same criminal by leveraging on the "trust" already built through the initial fraud scheme. CEF syndicates are regularly composed of well-educated and technically competent professionals. The following figure illustrates the CEF criminal structure.



There is also a rising link between CEF and human trafficking, where victims are lured through fake job ads to online call centres and forced to commit CEF on an industrial scale. This allows CEF syndicates to increase the geographical diversity of the online victims that they can target (as the

(Continued on page 15)

The 2023 Geography of Cryptocurrency Report

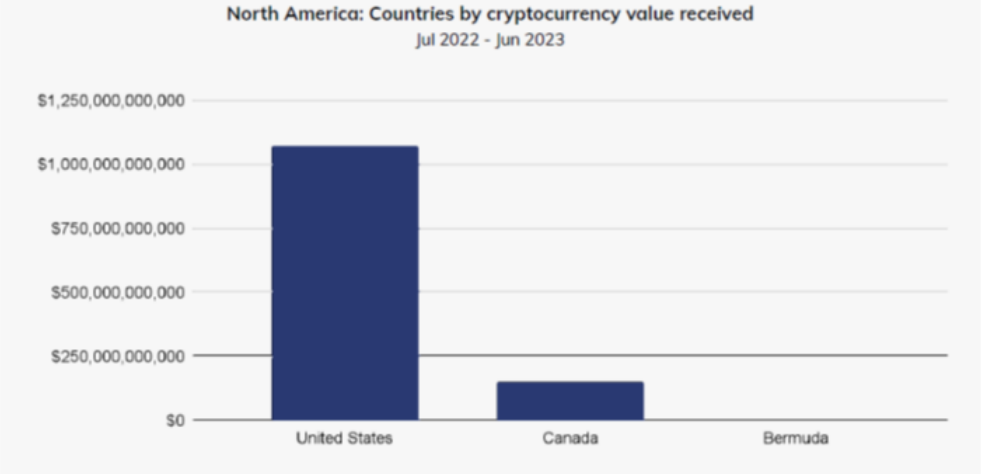
The **Global Crypto Adoption Index**, released October 23, 2023, is made up of five sub-indexes, each of which is based on countries' usage of different types of cryptocurrency services. The 155 countries are ranked for which '**Chainalysis'** has sufficient data according to each of those five metrics, take the geometric mean of each country's ranking in all five, and then normalize that final number on a scale of 0 to 1 to give every country a score that determines the overall rankings. The closer the country's final score is to 1, the higher the rank. ***Canada has an overall index ranking of 19.*** The five sub-indexes include:

1) On-chain cryptocurrency value received at centralized exchanges, weighted by purchasing power parity (PPP) per capita
2) On-chain retail value received at centralized exchanges, weighted by PPP per capita
3) Peer-to-peer (P2P) exchange trade volume, weighted by PPP per capita and number of internet users
4) On-chain cryptocurrency value received from DeFi protocols, weighted by PPP per capita
5) On-chain retail value received from DeFi protocols, weighted by PPP per capita.

The 2023 Global Crypto Adoption Index Top 20

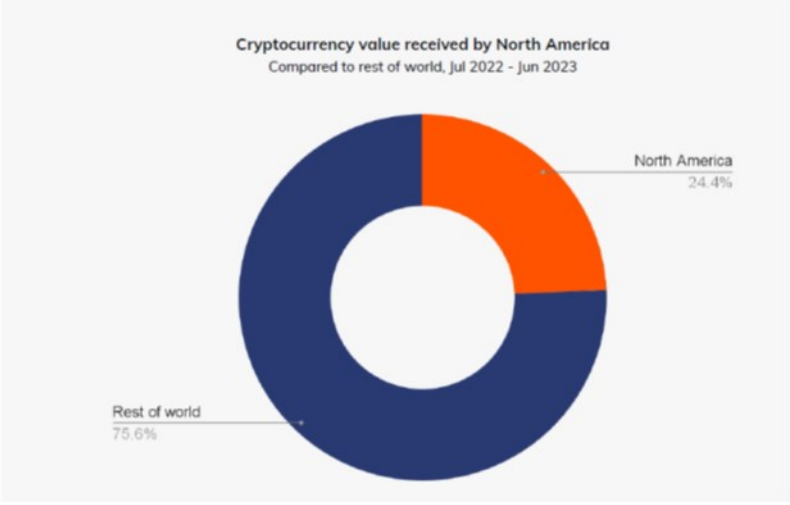
Country	Region	Overall index ranking	Centralized service value received ranking	Retail centralized service value received ranking	P2P exchange trade volume ranking	DeFi value received ranking	Retail deFi value received ranking
India	Central& Southern Asia and Oceania	1	1	1	5	1	1
Nigeria	Sub-Saharan Africa	2	3	2	1	4	4
Vietnam	Central& Southern Asia and Oceania	3	4	4	2	3	3
United States	North America	4	2	8	12	2	2
Ukraine	Eastern Europe	5	5	3	11	10	10
Philippines	Central& Southern Asia and Oceania	6	6	6	19	7	7
Indonesia	Central& Southern Asia and Oceania	7	13	13	14	5	5
Pakistan	Central& Southern Asia and Oceania	8	7	7	9	20	20
Brazil	Latin America	9	9	11	15	11	11
Thailand	Central& Southern Asia and Oceania	10	8	15	44	6	6
China	Eastern Asia	11	10	5	13	23	23
Turkey	MiddleEast& North Africa	12	11	9	35	12	12

Country	Region	Overall index ranking	Centralized service value received ranking	Retail centralized service value received ranking	P2P exchange trade volume ranking	DeFi value received ranking	Retail deFi value received ranking
Russia	Eastern Europe	13	12	10	36	9	9
United Kingdom	Central, Northern, & Western Europe	14	15	20	38	8	8
Argentina	Latin America	15	14	12	29	19	19
Mexico	Latin America	16	17	18	30	16	16
Bangladesh	Central& Southern Asia and Oceania	17	18	19	33	22	22
Japan	Eastern Asia	18	22	21	49	18	18
Canada	**North America**	**19**	**25**	**23**	**62**	**14**	**14**
Morocco	MiddleEast& North Africa	20	27	25	21	26	26
Country	**Region**	**Overall index ranking**	**Centralized service value received ranking**	**Retail centralized service value received ranking**	**P2P exchange trade volume ranking**	**DeFi value received ranking**	**Retail deFi value received ranking**



North America

North America is the largest cryptocurrency market studied, with an estimated $1.2 trillion in value received on-chain between July 2022 and June 2023. That total represents 24.4% of global transaction activity during the time period studied.



Source:
https://go.chainalysis.com/geography-of-cryptocurrency-2023.html

Europol Report: Fraud

Europol's first ever threat assessment on the topic, ***'The other side of the coin: an analysis of financial and economic crime in the EU'***, sheds a light on this system which, from the shadows, sustains the finances of criminals worldwide. The 58-page report analyzes financial and economic crimes affecting the EU, such as money laundering, corruption, fraud, intellectual property crime, and commodity and currency counterfeiting. Criminal actors involved in fraud schemes include both opportunistic individuals and criminal networks. They differ according to the type of fraud, their level of expertise, the targets chosen, and the tools and techniques that they use. Currently, most frauds are cyber-enabled.

Fraud offences use deceit for voluntary but unlawful transfer of money, goods, or undue advantages. Fraud schemes with a wide range of targets are present but under-reported, as victims seek to protect their name and reputation.

- The criminal actors engaged in fraud schemes span from opportunistic individuals to highly organized networks, with mid-level management layers and external criminal service providers with expertise in tax, banking, law, finance, IT, and money laundering. As a multitude of frauds are cyber-enabled, fraudsters are avid customers of cybercrime as-a-service, making use of tools and/or data on offer.
- Fraudsters either target large pools of potential victims or victimize selected targets. Re-victimization of targets is a common practice. Social engineering and impersonation are the most used techniques.
- The most common types of fraud include investment frauds (especially crypto-investments), business email compromise (BEC), e-commerce frauds, tech support frauds, romance frauds, and phishing campaigns.

Criminal networks operating frauds rely on technical knowledge and external criminal service providers with relevant expertise to help commit the crime. Fraudsters are knowledgeable about their targets, and use facilitators such as call centre operators, money mules, and cash couriers. Both EU and non-EU criminal networks engage in fraudulent schemes, frequently targeting victims speaking the same language but located far away, often across multiple countries. Money mules and money launderers are often located in other countries than the fraudsters.

Fraudulent schemes are increasingly run online using digital tools and techniques, although some types of fraud traditionally include face-to-face interaction between fraudsters and victims. Fraudsters increasingly use sophisticated and varied social engineering techniques to target potential victims—often based on their status, psychological conditions, and habits, as extensive information can be found online.

Impersonation is one of the main tools used in online frauds. Fraudsters impersonate bank officials, CEOs, legitimate businesses and vendors, IT officers, police officers, relatives, and acquaintances of victims.

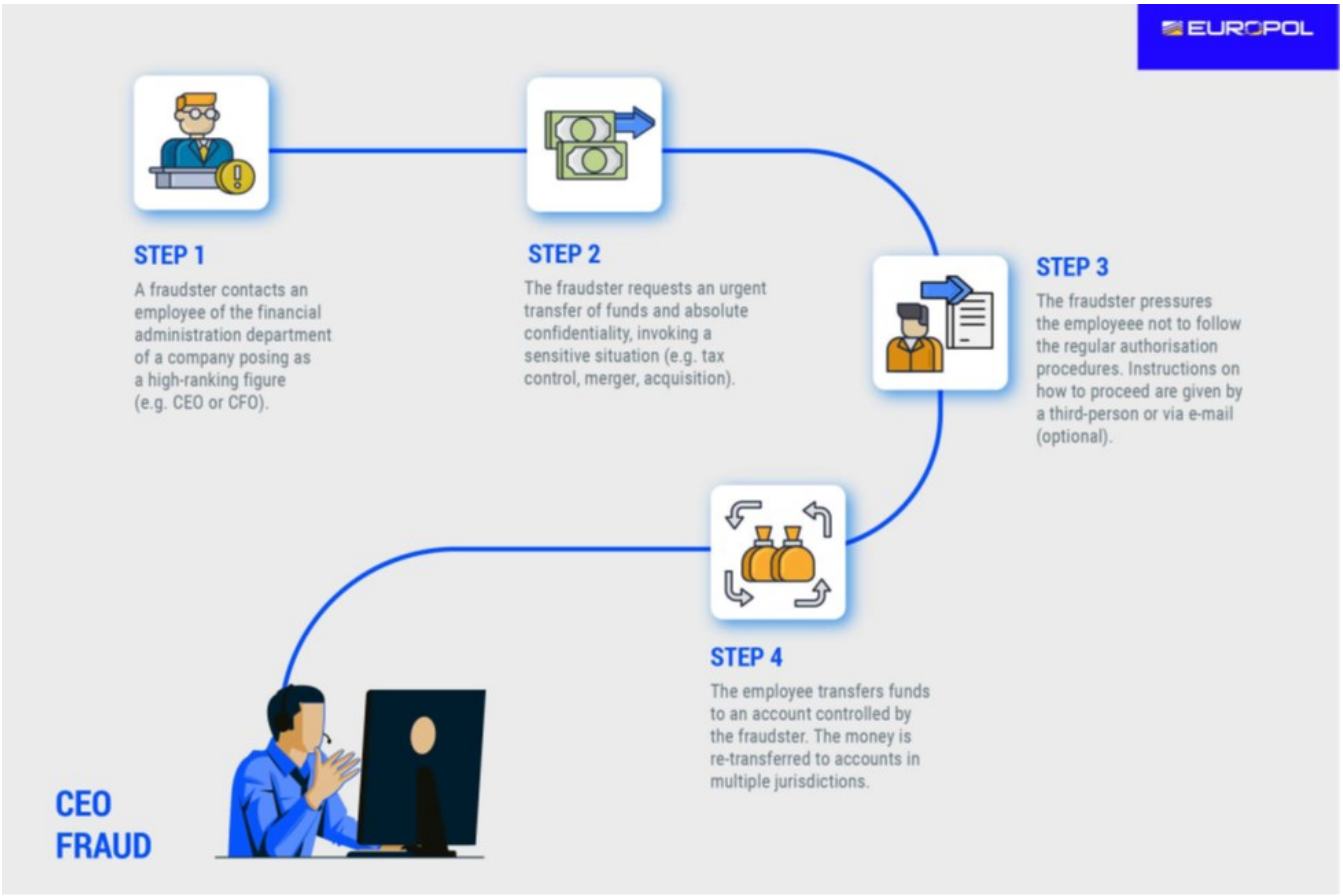
Investment Fraud: Investment fraud is a key threat in the EU, causing substantial losses for individuals and companies. The number of online investment fraud investigations reported to Europol has increased over the past two years, but victims remain reluctant to report the crime.

Case Example: A criminal network used the social media platform 'Vitae.co' and the website 'Vitaetoken.io' to trick people into investing in a cryptocurrency Ponzi scheme. Around 223 000 individuals from 177 countries are believed to have fallen victim to it. The members of this criminal network included Belgian nationals who used a company under Swiss jurisdiction. Over EUR 1 million in cash was seized, along with EUR 1.5 million in cryptocurrencies and 17 luxury vehicles (pg. 27).

Business e-mail compromise (BEC): Also called payment diversion fraud, BEC is a highly profitable fraud targeting EU private businesses and organizations that often operate internationally, perform wire transfers and have networks of suppliers. Chief executive officer (CEO) and fake invoice frauds represent the most

common BEC categories, particularly effective due to the combination of social engineering and sense of urgency transmitted to the victims. Criminals either hack the victims' email or send messages to the targets that appear to come from within the organization (usually a financial department, a manager or an employee) or from a business partner, making a request for a quick transaction with some sort of imperative justification (as an acquisition or a tax control, or the change of banking details), or asking to pay an invoice that looks genuine - but with the recipient's account modified by the scammers. Victims who follow the instructions may be wiring several transfers before realizing that it is a scam.

Social engineering plays a key role, as fraudsters use publicly available information about employees, direct collaborators, and business partners, among other things, to sound convincing. Phishing is often used to obtain personal and security data, enabling fraudsters to access and manipulate communication. BEC is often linked to subsequent investment and non-delivery frauds (when it involves fake invoices). Fake invoice fraud through impersonation often targets intellectual property (IP) owners throughout the application process, with fraudsters posing as competent IP offices (pg. 28).



Case Example: A criminal network composed of nationals from different African countries residing in the EU set up a sophisticated fraud scheme combining BEC and e-commerce fraud. The fraudsters faked email addresses and websites to impersonate legitimate wholesale companies and receive orders from other companies, mainly European and Asian. Advance payments were requested and the goods were never sent. Proceeds were laundered through Romanian bank accounts controlled by the criminals, then withdrawn at ATMs (pg.29).

Case example: In an online scam in 2022, fake correspondence was sent via email and social media, purportedly from Europol departments and senior staff. The message told victims that they had visited websites hosting child sexual abuse material, and urged them to reply to an email address. Respondents were asked to make a payment between EUR 3,000 and 7,000 via bank transfer or instant money services to avoid prosecution (pg. 30).

Case example: Food Fraud - A two-part investigation across several EU member states unveiled a criminal network involved in food fraud. In 2023, 27 suspects were arrested for relabelling millions of expired food products and reintroducing them into the supply chain. They acquired immense quantities of expired food and beverages and would chemically erase the expiry date and reprint a new one, or forge new labels. The suspects are believed to have made at least EUR 1 million in profits (pg. 30).

Case example: In October 2021, Europol launched operation SENTINEL to counter criminal activities threatening the Next Generation EU recovery fund, particularly fraud, corruption, embezzlement, misappropriation and money laundering. Irregularities and crimes are investigated by the 21 EU member states participating, either under their national competences or by the European Public Prosecutor's Office (EPPO), Eurojust, and the European Anti-Fraud Office (OLAF), in accordance with their respective legal framework (pg. 32).

Read more: other examples provided included: e-commerce fraud; tech support fraud, romance fraud, recovery or refund scam, mass mailing fraud, food fraud, subsidy fraud, and illicit cigarette fraud.

Source:
https://www.europol.europa.eu/media-press/newsroom/news/new-europol-report-shines-light-multi-billion-euro-underground-criminal-economy

Cybercrime Money Laundering Red Flags

Cybercrimes often exhibit 'red flag' characteristics that can assist businesses in detecting and preventing money laundering, thereby enhancing their compliance management controls.

Since the COVID-19 pandemic, cybercrime has increased by 600 percent. The Financial Crimes Enforcement Network (FinCEN) released a series of advisories calling financial institutions to be particularly vigilant for red flags that indicate cybercrime money laundering, including:

- Unusual transactional behavior such as suddenly increased frequencies or volumes of online transactions.
- Online transactions involving parties located in high-risk countries.
- Recently opened online accounts that receive large deposits or conduct large transactions that are inconsistent with the customer's profile or account history.
- A high number of payments made with prepaid cards or with virtual currencies such as Bitcoin.
- Correspondence sent to or from customers that indicate phishing attempts, frequent misspellings in the text of correspondence, or suspicious address credentials.
- Email or social media solicitations for fraudulent charity donations.
- Charitable organizations that do not have an in-depth history or cannot be independently verified as legitimate organizations.

Beyond Our Borders

Somalia

CAPITAL: Mogadishu;

GDP: USD 7,628.00 Million;

INCOME GROUP: Low Income;

POPULATION: 17,065,581;

GEOGRAPHY TYPE: Coastal

Somalia is located in the Horn of Africa, It is bordered by Ethiopia to the west, Djibouti to the northwest, the Gulf of Aden to the north, the Indian Ocean to the east, and Kenya to the southwest.

The U.S. *International Narcotics Control Strategy Report* (INCSR - 2019) no longer lists Somalia as a *country of primary concern* for money laundering. Canada has sanctions and related measures against Somalia (2019) for arms and related material embargo, asset freeze, export and import restrictions and technical assistance prohibitions.

The *2023 Basel Index* covers 152 jurisdictions and is based on the assessment of the quality of countries' anti-money laundering and countering the financing of terrorism (AML/CFT) frameworks and related factors such as financial sector standards, public transparency, corruption and rule of law. The scores range from 0 (low risk) to 10 (high risk) and provide an overall score of countries' money laundering/ terrorism financing risk. The *Basel Anti-Money Laundering (AML) Index Report 2023* did not rank Somalia.
https://baselgovernance.org/sites/default/files/2023-11/Basel%20AML%20Index%202023%2012th%20Edition.pdf

CORRUPTION: As a matter of policy, the government does not encourage or facilitate the illicit production or distribution of narcotics, psychotropic drugs, controlled substances, or the laundering of proceeds from illegal drug transactions. Transparency International's *Corruption Perceptions Index* (CPI) released in 2023, which measures "the degree to which corruption is perceived to exist among public officials and politicians"; rated Somalia as one of worst countries with a score of 12/100 with a ranking of 180th compared to Canada's score of 74/100 and ranking of 14th out of the 180 countries and territories included in the index.
https://www.transparency.org/en/cpi/2022

Criminality

CRIMINALITY SCORE: 6.13. 45th of 193 countries, 13th of 54 countries in Africa, and 6th of 9 countries in East Africa.

PEOPLE: Human trafficking continues to be a significant area of concern in Somalia. Men, women, and children are regularly subjected to forced labour and sex trafficking. Somalia is a primary source country for human smuggling, with many people being smuggled across East Africa to Libya and then on to Europe. Somalia is also a prominent transit hub for Ethiopian individuals smuggled. Smuggling networks move people, often on a cyclical basis, with little effective resistance from the state. Extortion and protection racketeering are a major source of income for terrorist groups such as Al-Shabaab and ISIS-Somalia. Citizens, companies, NGOs, and humanitarian organizations often pay extortion fees to these groups to protect their personnel and physical assets. The taxation of trucks and cars moving through checkpoints is considered one of the most lucrative sources of extortion for Al-Shabaab.

TRADE: There is a substantial number of illegal weapons in Somalia, ranging from pistols to machine guns, and these are commonly trafficked by clan militias, Al-Shabaab, governmental groups, and transnational trafficking networks based in the north, particularly Puntland and eastern Somaliland. The country is affected by transnational organized crime, in the form of piracy, human trafficking, and drug trafficking, leading to an increased demand for the illicit supply of weapons. Pharmaceutical products are the most commonly circulated counterfeit items in Somalia.

ENVIRONMENT: The illegal trade of flora in Somalia remains

a prevalent problem, with illegal charcoal trade being the most prominent form of flora crimes. Fauna crime is a moderate criminal market in Somalia. Cheetah cubs are trafficked from Ethiopia, through Somaliland, and on to Saudi Arabia or the United Arab Emirates, where they are in high demand as novelty pets. The smuggling of live big cats is also linked to internal issues within Somalia; farmers are known to capture cheetahs to sell as a way of redeeming losses resulting from the cheetahs attacking their cattle. In terms of illegal, unreported, and unregulated fishing, Somalia is seriously affected, with foreign nationals driving the trade.

DRUGS: There is no notable domestic heroin market in Somalia, despite its location on the southern route for smuggling opiates from Afghanistan. Somalia has a volatile and continually shifting security environment, which makes the transit of narcotics difficult.

CYBER-CRIMES: Al-Shabaab limits the use of information and communications technology and prohibits internet usage in the regions under its control, where rules and regulations are difficult to enforce.

FINANCIAL CRIMES: Somalia does not have a strong financial regulation structure, and financial crime is widespread. Al-Shabaab is one of the primary actors, owing to its independent funding mechanisms and administrative bureaucracy. The group is known to divert and misuse international relief funds intended for famine victims. Other types of financial crime prevalent in Somalia include fraud and embezzlement, especially fraudulent financial activity and the manipulation of procedures linked to procurement.

CRIMINAL ACTORS: In Somalia, Al-Shabaab operates as part of a larger transnational criminal enterprise, engaging in illicit trafficking, extortion, and racketeering. The group has infiltrated many areas of Somali society and regularly commits serious abuses, including forcibly recruiting adults and children, and extorting so-called taxes through threats. Al-Shabaab operates a network of checkpoints on roads across southern and central Somalia and collects taxes on various goods. Iranian-made weapons have been smuggled into the country, a trade that involves multiple armed groups and clans, while sophisticated transnational maritime trafficking networks operate to smuggle small arms and light weapons from Iran, Yemen, the United Arab Emirates, and Oman. Turkey and Qatar are also involved in Somali politics and have faced allegations of supporting radical Islamist groups and being responsible for human rights abuses. Foreign private military contractors, including some hired by Eritrea, contribute significantly to violence and security distortions in Somalia.

Resilience

RESILIENCE SCORE: 1.79. 187th of 193 countries, 52nd of 54 countries in Africa, and 9th of 9 countries in East Africa.

LEADERSHIP & GOVERNANCE: Somalia is a fragmented country and continues to be characterized by internal tension, violent extremism, extensive displacements, and weak governance. Corruption, a disillusioned youth, and the privatization of public goods by militia leaders and warlords remain major challenges in the promotion of peace and stability. In fact, Somalia is considered to be one of the most fragile and corrupt states in the world, and corruption is facilitated by dysfunctional institutions.

CRIMINAL JUSTICE & SECURITY: The formal court system in Somalia is highly corrupt and dysfunctional. Access to justice is low, and the formal justice system faces challenges and criticism from Sharia leaders as well as others delivering customary law at the local level, including Al-Shabaab. Military courts are still used throughout Somalia to try civilians, primarily those suspected of being members of terrorist groups. Prisons are overcrowded, as many inmates are held on remand for numerous years before trial. The Somali government has limited control over the country's territory, with different regions operating as de facto independent states or under the control of armed groups. The country's borders are porous, and smuggling activities are widespread. Al-Shabaab conducts cross-border attacks into Kenya, exacerbating the already tense relationship between the two countries.

ECONOMIC & FINANCIAL ENVIRONMENT: The Central Bank of Somalia recently issued the country's first mobile money licenses and set up a national payments system, but anti-money laundering controls have not been implemented. A robust informal money system, known as hawala, serves the vast Somali diaspora, enabling transactions to flow across borders without surveillance. Money transfer operators do not have robust anti-money laundering infrastructure, meaning that most transactions occur outside of what the formal financial system has the capacity to regulate. The absence of a regulatory framework and business infrastructure, along with a

largely privatized banking system, hampers the state-regulated economic environment. As a result, Somalia is considered among the worst performing countries in the world by most relevant economic and businesses indicators.

CIVIL SOCIETY & SOCIAL PROTECTION: The central state has essentially no capacity to provide basic services, and is reliant on the provision of food, shelter, and medical supplies from the international community. The distribution of aid is politicized, with Al-Shabaab taxing such funds to reinforce its local power. Somalia is one of the most dangerous countries in the world for journalists, with political violence and corruption undermining the freedom of the press.

(Cyber-Enabled Fraud - Continued from page 7)

trafficked victims can be exploited for their knowledge of languages and cultural insight). It can also increase the sophistication of CEF centres by trafficking skilled professionals such as information technology workers or "digital sales executives". These call centres sometimes intentionally operated within the time zones of intended victims, and used rental properties for temporary criminal operations, which allowed them to quickly re-locate and change IP addresses to avoid law enforcement detection.

In conclusion, CEF is perpetrated by transnational, organized crime syndicates. The scale and magnitude of CEF is expected to grow with the rising trend of digitalization and virtual services across the globe. Jurisdictions should also be aware of the additional vulnerabilities across various sectors, including digital financial institutions and non-traditional sectors, that criminals may exploit to enhance CEF and ML techniques through growing digitalization. CEF can have significant and crippling financial impact on victims. But the impact is not limited to monetary losses; it can have devastating social and economic implications. The conclusions of this report indicate three priority areas in which jurisdictions should act to tackle CEF and related ML more effectively: (i) enhancing domestic co-ordination; (ii) supporting multilateral collaboration; and (iii) strengthening detection and prevention.

Source:
https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

Case Study: Transnational Organized Crime

This multi-year investigation focused on a narcotics trafficking and money laundering organization with ties to the Sinaloa and Jalisco New Generation cartels. The investigative efforts included the analysis of over 100 Bank Secrecy Act (BSA) records that helped lead to numerous arrests and the significant disruption of this criminal organization. DEA agents identified members of a global money laundering network that controls the flow of narcotics proceeds for Mexican cartels. Investigators leveraged this information to target the money laundering cells providing acquisition and processing of funds, and in under 9 months, investigators seized over $2 million and the largest volume of fentanyl in U.S. history.

Investigators subsequently carried out numerous operations, which provided a plethora of new leads to DEA offices located domestically and internationally. These operations helped initiate a large-scale financial investigation into multiple companies based in the U.S., Mexico, China, Taiwan, Hong Kong, Italy, and France. An analysis of the financial activity of these companies revealed that many of their accounts were used to transfer narcotics proceeds to various parts of the world before returning to the Mexican cartels. This financial investigation included an analysis of a high volume of BSA data, and resulted in the discovery of accounts holding hundreds of millions of dollars in forfeitable and verifiable narcotics proceeds intended to be used for real estate and other investments in an attempt to legitimize the funds. Investigators subsequently seized over $22 million from a Miami-based real estate investment firm that was using sophisticated trading techniques to repatriate narcotics proceeds to Mexico through U.S.-based real estate purchases. Investigators also discovered numerous accounts invested in corporate bonds, treasury notes, and various stock indexes. Seizures of these account totaled nearly $85 million.

Investigators continue to develop the "end game" scenario involving the arrest of numerous money launderers and brokers working for the Mexican cartels as well as the global money laundering network. To date, the investigation has resulted in the combined seizure of 562 kilos of narcotics and $165 million in criminal proceeds, as well as the execution of 162 arrests and indictments of 25 organization members.

Source: https://www.fincen.gov/news/news-releases/fincen-recognizes-law-enforcement-cases-significantly-impacted-bank-secrecy-act