The Business Crime Solution

Helping Build Practical Compliance Strategies

September 2021

Training

The Impact Is Evident from the Plan

This month, ABCsolutions' professional certification institute, CAMLI, held another one of its successful webchat sessions. Compliance officers love to learn from each other, exchange ideas with each other, really listen to one another, and compliment each other when an idea, practice, or thought touches the 'get excited' nerve. Wednesday, September 15th was a perfect example of all those things coming together in 65 minutes of shared enjoyment.

This CAMLI webchat was all about the 'Training Plan', which is now required by FINTRAC as one of the pillars of an effective Compliance Program. Now training plan requirements are not a new task for most financial institution reporting entities, but for many other reporting entities, MSBs, accountants, precious metals and gems dealers, and notaries, that is not the case. The training plan has caught them off guard and many businesses in those sectors have a way to go before their plans become an integral part of their annual compliance management activities.

So, what did we learn from the webcast seminar? First and foremost, the depth to which financial entities go to structuring the various required and spontaneous training activities across their organization. Examples of record-keeping spreadsheets were shared, with each employee and manager assigned to those training sessions most representative

(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**

A Word from the Editors

In this month's issue, we take a closer look at the series of regulatory, guidance, and operational alert updates from FINTRAC that recently were released or came into force. Take note of the changes regarding terrorist property, the 24-hour rule, and third party determination as they will have a direct impact on your organization's reporting practices.

Also, a quick reminder that registration for Money Laundering in Canada 2021 will remain open until Friday, October 22. Make sure to mark your calendar if you are planning to participate in this event.

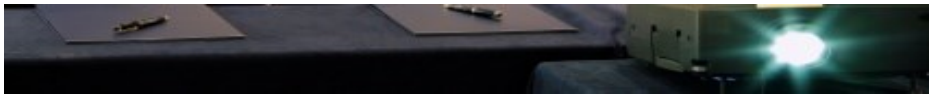
Upcoming Events:

October 25 - 27, 2021

DATE CHANGE

Money Laundering in Canada 2021

https://www.moneylaundering.ca/public/events/mlincanada/2021/index.php



In This Issue:

CAMLI Training Program

Managing Your Risks: Elder Financial Abuse/ Exploitation

Visit our website for more information

www.camli.org

Next Month:

- ⇨ 2021 Basel Index
- ⇨ Crime Statistics

In the News

Four Ontario Residents Face Charges related to COVID-19 Funds

Four people are now facing criminal charges in connection with an alleged embezzlement scheme that is said to have defrauded $11 million in COVID-19 relief funds from the Ontario government.

The OPP reported began the investigation into the scheme in August 2020 after receiving a referral from the Ontario Ministry of Education.

"The size and scope of this fraud was significantly more complex than first identified," the OPP said in a statement.

Sanjay and Shalini Madan – Sanjay Madan was a senior IT role in the Ontario government and helped develop a computer app related to COVID-19 Relief Benefit. The Ontario government has sued Mr. Madan, his wife, and two adult children for allegedly issuing and banking cheques illegally under the Support for Families program. Ontario has also accused Madan of taking millions in kickbacks in an alleged fraud worth more than $30 million.

- Accused by the province of embezzling $11 million in Covid-19 relief funds.
- Faces two counts of fraud over $5000 and two counts of breach of trust.
- Charged with laundering proceeds of crime of $5000 and possession of the proceeds of crime over $5000

In a statement of defence filed in Superior Court, Madan blames the province for allegedly lax security measures that allowed "widespread misappropriation" of the COVID-19 relief funds.

A court injunction has frozen $28 million in Madan family assets, including: $12.4 million in Indian bank accounts; an $8-million Waterloo apartment complex; a seven-bedroom house in North York valued at $2.57 million; and six Toronto condominiums valued at about $3 million.

Vidhan Singh - The Ontario government alleged that Singh paid Sanjay Madan $5 million in commissions for government contracts. Sanjay Madan allegedly received commissions of $10 million for steering government consulting contracts to compa-

(Continued on page 6)

FinCEN to Add Antiquities Industry to List of Regulated Sectors

In late September, the Financial Crimes Enforcement Network (FinCEN) issued an *Advance Notice of Proposed Rulemaking* (ANPR) to gather input from stakeholders. The notice was in reference to adding Antiquities trading to the Bank Secrecy Act (BSA) as was directed by Congress. FINCEN is beginning the process of creating proposed rules for this sector and the ANPR is one step in the process.

"The trade in antiquities may be exploited by money launderers and terrorist financiers to evade detection by law enforcement and to launder their illicit funds through the U.S. financial system. Terrorist organizations, transnational criminal networks, and other malign actors may also seek to exploit antiquities to transfer value to acquire new sources of funds, evade detection, and launder proceeds from their illicit activities. Some terrorist groups have generated revenue from permitting or facilitating the illegal extraction or trafficking of antiquities in territories where they operate."

FINCEN is looking for input on a variety of elements including: how to define "antiquities"; who should be covered by the regulations (buyers, dealers, agents etc.); are there exemptions that would be appropriate; and recommended pricing thresholds for reporting. Feedback is due by October 25, 2021

Sources:
https://www.fincen.gov/news/news-releases/fincen-launches-regulatory-process-new-antiquities-regulations

https://www.federalregister.gov/documents/2021/09/24/2021-20731/anti-money-laundering-regulations-for-dealers-in-antiquities

https://www.theartnewspaper.com/2021/09/25/antiquities-trade-should-prepare-for-more-government-oversight

https://www.wsj.com/articles/u-s-solicits-public-feedback-on-anti-money-laundering-rules-for-antiquities-dealers-11632422996

(Front Page - Continued from page 1)
of what they do for the business. Duplication was only evident when knowledge was common to everyone and essential as a backdrop to other learning requirements.

Learning success was a primary indicator for compliance officers of how well their plan and training activities were achieving the organization's goals. Webchat participants spontaneously reinforced the importance of testing what each individual had learned. Pass scores were all set and failure to reach those levels forced the employee to circle back to the problem content, review it, and test again. Several, participants jumped into the conversation at that point to stress the importance of using training solutions that randomized the choice of questions every time an employee retested. Platforms without that feature were viewed as unreliable when it came to knowledge retention and the confidence in the training to meet its stated capabilities.

Training plans need to pay attention to spontaneous learning opportunities as well. The response to this fact pushed many of those participating in the webchat to build robust information-sharing platforms that get the learning out to the target groups needing it the most, with sign-off processes that enabled compliance officers to confirm that everyone targeted had read the content.

A number of the participants expressed interest in these different processes and spoke of plans to approach their own training group to consider implementing similar procedures. Imitation is a strong form of flattery, and our Wednesday group was not shy to publicly share that kind of praise.

To me, as a lifelong educator, to see the degree of complexity, thoroughness, and advanced thinking put in by compliance officers keen on making sure their colleagues keep on top of what needs to be done and what their specific role in the compliance program is, was extremely rewarding. These individuals truly "get it" in my book and their willingness to share what they have learned is a bonus. For 20+ years, compliance officers have often struggled to convince management that an AML/CTF compliance management program is only as good as the activities, approaches, and reliability testing incorporated into its design and delivery. Sounds like those senior managers are getting the message and have become believers by providing the resources to access the programs designed for these goals. Well done! For those who missed the chat, join in next time, there are many great practices yet to be shared.

Legislative Updates – Reporting terrorist property to FINTRAC

You must submit TPRs to FINTRAC electronically by fax if you have the technical capability to do so. If you do not have the capability to submit by fax, you must send the report by mail. FINTRAC's TPR form can be printed from the reporting forms web page, or you can request a form to be faxed or mailed to you by calling FINTRAC at 1-866-346-8722. There is no official acknowledgment of receipt when you submit a TPR to FINTRAC.

Submit a TPR by fax to: 1-866-226-2346

Submit a TPR by mail through regular or registered mail to:

Financial Transactions and Reports
Analysis Centre of Canada
Section A
234 Laurier Avenue West, 24th floor
Ottawa ON K1P 1H7

Terrorist Property Report + submit STR: If a transaction was attempted or completed, and it involved property that you know is owned or controlled by or on behalf of a terrorist group, or that you believe is owned or controlled by or on behalf of a listed person (for which you must submit a TPR), you should also submit an STR to FINTRAC because you have reached the threshold of reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a terrorist activity financing offence.

Reasonable grounds to suspect means there is a possibility that an ML or TF offence has occurred based on an assessment of facts, context, and indicators, and you are able to present the reasons why it is suspicious without proof or verification. Having reasonable grounds to believe is a higher threshold and means there is a probability that an ML or TF offence has occurred, and you are able to present a set of verified facts that can be proven and that support this belief.

FINTRAC Issues Operational Alert Update:

Laundering of Proceeds from Human Trafficking for Sexual Exploitation

Human trafficking for sexual exploitation is reported to be more prevalent than forced labour. Canada is a source, transit, and destination country for men, women, and children trafficked for the purposes of sexual exploitation. Traffickers exploit their victims primarily for financial gain.

Research suggests that human trafficking for sexual exploitation, like drugs and weapons trafficking, is just another commodity in a range of criminal activities perpetrated mostly by organized crime groups who often collaborate with each other to maximize illicit financial gain. Sexual exploitation is a high-value business for criminals because, unlike a drug that can only be sold once, a human being can be sold repeatedly over an extended period of time. This type of crime is also attractive to criminals because the risk of losing business due to detection and successful prosecution is kept low through coercion of their victims in combination with the use of well-known money laundering methods. As a result, the perpetration of this crime is reinforced because criminals are able to benefit from the illicit proceeds. *The International Labour Organization (ILO) estimates that global proceeds from human trafficking amount to USD 150 billion per year with USD 99 billion sourced specifically from forced sexual exploitation*.

Project Protect is a public-private partnership initiative led by the Bank of Montreal, supported by Canadian law enforcement agencies and FINTRAC. First launched in 2016, Project Protect targets human trafficking for sexual exploitation by focusing on the money laundering aspect of the crime. The objective of the project is to improve the collective understanding of the crime, and to improve the detection of the laundering of proceeds from human trafficking for sexual exploitation.

FINTRAC Analytics:

Locations where this activity occurred:

- At short-stay locations (e.g., hotels); illicit storefront businesses offering sexual services (e.g., spas, massage parlours, private clubs); and at private residences (e.g., apartments) with some crossover between these three categories. All used advertisements of escort services to obtain clients and some traffickers operated their own escort agencies.

About the Victims:

- Overall, victims were nearly all females and 60% were under 25 years old at the time of their transactions and some were minors.

About the Traffickers:

- Traffickers were mostly males aged between 24 and 36 years old. Female traffickers were mostly aged between 27 and 32 years old, although most were also victims and connected to male traffickers.
- Traffickers who exploited their victims out of private residences or in illicit storefront businesses offering sexual services were mostly older females (usually over 40 years old) and many operated with their spouses.
- Many traffickers were also involved in or suspected to be involved in other criminal activities (e.g., drug trafficking, fraud) and were members or associates of criminal groups.
- Many traffickers used their victims to conduct other crimes. Therefore, the money laundering methods observed were likely also used to launder proceeds generated from other criminal activities and are not necessarily specific to human trafficking.

Money Laundering Methods:

- Several **money laundering methods** were identified, including the use of online casinos, casinos, virtual currencies, gift cards, nominees, front companies owned by traffickers or their associates, funds layered between related accounts, and investment accounts, and prepaid credit cards in which traffickers and victims used to launder funds and to pay for human trafficking-running costs (e.g., escort ads, hotel bookings).
- Traffickers frequently used nominees to funnel proceeds of crime, pay for human trafficking running costs, launder funds, or conceal beneficial ownership. These nominees were often victims and family members of traffickers. Victims were used as intermediaries to funnel funds to traffickers and other victims.
- Traffickers and victims often purchased virtual currencies with funds sent directly to virtual currency exchange businesses sometimes doing so immediately after receiving several email money transfers from third parties. However, several traffickers and victims also sent email money transfers to individuals who purchased virtual currencies on behalf of others. One such individual advertised their intermediary virtual currency services on escort websites.
- Front businesses were used to illicitly offer sexual services, to launder proceeds, and/or to manage the running costs associated with human trafficking. For example, illicit proceeds were used to pay the rent and utilities for residential properties where sexual services are rendered or used as safe houses. Front companies in FINTRAC's sample were diverse and included industries such as, music, spas, salons, restaurants, motels, farming, IT services, clothing, vehicle and construction-related businesses, and transport businesses among others. Front companies *co-mingled legitimate* with illicit funds and/or had limited business-related transactions. They were owned by traffickers, their associates and other members of their human trafficking networks including some victims. Businesses owned by victims also transferred funds to traffickers and their businesses.
- International funds transfers were primarily *outgoing* from Canada to countries such as the Philippines, Brazil, Russia, Portugal, China, Australia, Colombia, Taiwan, United States, Kazakhstan, United Arab Emirates, Hong Kong, South Korea, and Uzbekistan with reasons for transfers usually not provided.
    - Some outgoing transfers cited reasons mostly related to family, gift, loan repayments, or tuition.
    - Some funds transferred (totalling CAN$1.5 million) to the United States were cited as purchases of a hotel franchise – the sender of these transfers was a sex trade worker closely associated to traffickers. A different trafficker owned motel franchises in Canada as well.
- *Incoming* international funds transfers to Canada originated mostly from China but also from Hong Kong and South Korea and cited reasons such as living expenses, consulting, training, education and travel.

Source: https://www.fintrac-canafe.gc.ca/intel/operation/oai-hts-2021-eng

(Headlines - Continued from page 3)

nies controlled by Singh or himself. Singh has a court date on November 18th to face these criminal charges.

- Charged with fraud over $5,000, money laundering and possession of property obtained by crime over $5,000.

Manish Gambhir

- charged with possession of an identity document and possession of property obtained by crime.

"OPP spokesman Bill Dickson says the arrest is part of the same investigation that led to the arrests of a former bureaucrat, his wife, and a third man earlier this month."

Sources:
https://www.cbc.ca/news/canada/toronto/toronto-covid-relief-fund-1.6185794

https://www.cbc.ca/news/canada/toronto/ex-bureaucrat-accused-of-embezzling-covid-19-funds-from-ontario-government-now-facing-criminal-charges-1.6181943

https://www.thestar.com/politics/provincial/2021/09/30/opp-charge-fourth-person-in-connection-with-alleged-11m-theft-of-provincial-covid-19-relief-funds.html?rf

https://www.cp24.com/news/fourth-person-charged-in-alleged-embezzlement-of-ontario-covid-19-relief-fund-1.5606553

Legislative Updates: FINTRAC Interpretive Policy 24-Hour Rule

QUESTION	ANSWER
Will the requirement to aggregate multiple transactions over $10,000 that occur in a 24-hour period be delayed beyond June 1, 2021 for large cash transaction reports (LCTRs)?	FINTRAC has published guidance on the amendments to the 24-hour rule under the amended PCMLTFR. Please note that the updated guidance includes the following disclaimer: *This guidance on the 24-hour rule explains the requirements under the PCMLTFR that are in effect as of June 1st, 2021. From June 1st, these obligations will apply only to the reporting of large virtual currency transactions.* *The obligations will apply to large cash transactions, electronic funds transfers, and casino disbursements when FINTRAC updates the report forms for those transactions. Until then, reporting entities should continue to apply the 24-hour rule as outlined in FIN 4 (pre-June 1, 2021). https://www.fintrac-canafe.gc.ca/guidance-directives/overview-apercu/FINS/2009-08-31-eng* *Further details can be found in the Notice on forthcoming regulatory amendments and flexibility and the message concerning FINTRAC's Implementation of Regulatory Amendments. This page will be updated to include additional information as the revised report forms become available.* *During this time, REs are expected to be updating their processes, as well as, their policies and procedures to ensure compliance with the amended obligations.*
Clarify what is meant by "beneficiary" for aggregation under the 24-hour rule for large cash transaction reports (LCTRs) and electronic funds transfer (EFT) reports? Define 'beneficiary' vs. 'on behalf of'	*The person or entity that conducts the cash transaction or requests the initiation of the electronic funds transfer is the conductor of the transaction. The conductor of the transaction may or may not also be the beneficiary of the transaction.* *To clarify, FINTRAC's Guidance Glossary includes the following definitions of 'beneficiary' and 'on behalf of':* • *Beneficiary - A beneficiary is the individual or entity that will benefit from a transaction or to which the final remittance is made.* • *Third Party [also known as "on behalf of party" and "instructing party"] - Any individual or entity that instructs another individual or entity to act on their behalf for a financial activity or transaction.*

Please note: Post June 1st

A reporting entity (RE) must **not combine aggregation types**. The RE must determine who the relevant parties to a transaction are and then determine if, within a 24-hour period, there are reportable transactions based on the same conductor, third party (on behalf of), or beneficiary in accordance with their 24-hour rule obligations.

Provided Scenario #1 24-hour	Parties to the transaction	Pre-June 1st Reporting Obligation	Post-June 1st Reporting Obligation
1. Person A deposits 3 transactions within a 24-hour period: • $3000 into account of Person B • $4000 into account of Person C • $4000 into account of Person D	• Person A is the conductor of $11,000 worth of cash deposits; • Person B, Person C, and Person D are each a beneficiary; and • there does not appear to be a third party.	LCTR required because the RE knows, pursuant to paragraph 3(1)(a) of the current PCMLTFR, that the cash deposits were within a consecutive 24-hour period, collectively total more than $10,000 CAD, and are all conducted by the same person, Person A.	LCTR required because the RE knows, pursuant to subsection 126(a) of the amended PCMLTFR, that the cash deposits were within a consecutive 24-hour period, collectively total more than $10,000 CAD, and are all *conducted* by the same person, Person A.

Provided Scenario #1 24-hour	Parties to the transaction	Pre-June 1st Reporting Obligation	Post-June 1st Reporting Obligation
2. Person E receives 3 cash deposits into their account(s), each conducted by different people: • $3000 from Person F • $4000 from Person G • $4000 from Person H	• Person E is the beneficiary of $11,000 worth of cash deposits; • Person F, Person G, and Person H are each a conductor; and • There does not appear to be a third party.	LCTR not required as there is no requirement in the current PCMLTFR to aggregate transactions based on the beneficiary of a cash transaction.	LCTR required because the RE knows, pursuant to subsection 126(c) of the amended PCMLTFR, that the cash deposits were within a consecutive 24 hour period, collectively total more than $10,000 CAD, and are for the *same beneficiary*, Person E. However, measure #2 of the Notice will delay the enforcement of the obligation to aggregate transactions based on the beneficiary for the LCTR and EFTR until the updated reporting forms are implemented. Therefore, FINTRAC will not expect an LCTR to be reported for this transaction if it occurs after June 1, 2021, but before the updated reporting form is available.

Provided Scenario #3 24-hour	Parties to the transaction	Pre-June 1st Reporting Obligation	Post-June 1st Reporting Obligation
3. Person A deposits 1 transaction of $3000 into their own account & Person B deposits $8000 into Person A's account	• Person A is the conductor and beneficiary of the $3,000 deposit; • Person B is the conductor of the $8,000 deposit; • Person A is also the beneficiary of the $8,000 deposit, and • There does not appear to be a third party.	LCTR not required as there is no requirement in the current PCMLTFR to aggregate transactions based on the beneficiary of a cash transaction.	LCTR required because the RE knows, pursuant to subsection 126(c) of the amended PCMLTFR, that the cash deposits were within a consecutive 24-hour period, collectively total more than $10,000 CAD, and are for the *same beneficiary*, Person A. However, measure #2 of the Notice will delay the enforcement of the obligation to aggregate transactions based on the beneficiary for the LCTR and EFTR until the updated reporting forms are implemented. Therefore, FINTRAC will not expect an LCTR to be reported for this transaction if it occurs after June 1, 2021, but before the updated reporting form is available.

FINTRAC still expects REs to obtain and report information regarding all applicable parties to a transaction (conductor, third/instructing party, and beneficiary, where possible), and to keep the applicable records.

...You Asked

Is an entity considered to be dealing in virtual currency (VC) if it operates VC ATMs? What information needs to be provided when registering with FINTRAC?

A person or entity that operates a VC automated teller machine (ATM) that allows clients to exchange fiat currency for VC or VC for fiat currency is engaged in VC exchange services and is required to register with FINTRAC as an MSB. Effective June 1, 2020, persons and entities dealing in VC are money services businesses (MSBs). Persons and entities dealing in VC include both VC exchange and VC transfer services.

In addition, there is no exemption under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) or its associated Regulations for MSBs who limit transactions to less than $1,000 CAD. An MSB who chooses to limit transactions to $999 CAD or below is still subject to all applicable obligations under the PCMLTFA and its associated Regulations, including the obligation to have a compliance program, to report suspicious transactions, etc.

Finally, should all the VC ATMs be owned by the same legal entity then each location should be entered as a branch of the business.

A Couple of Interesting Facts About the Source of Laundered Funds for Real Estate

Global Financial Integrity (GFI), the Washington, DC-based anti-corruption organization, found in a recent study that significant cash is laundered through real estate in Canada. What has proven to be interesting is the fact that Canada is the country where most of the laundered funds originated. Specifically, the study revealed 48.6% of cases involved Canadian-sourced funds being laundered. International sources were most often from China and the US. The largest international source was China, representing 22.9% of cases — about half as many as Canadian-sourced laundering. The US was third with 11.4%, half the size of China; followed by the Republic of the Congo at 11.4% Remember, this is in the context of the study and major cases where people were caught.

Primary Sources for Laundering the Dirty Cash

GFI found in its research that most of the money laundering is done through company structures, used in 51.4% of the cases. Third-party processing (45.7% of cases) and mortgage schemes (34.3%) round out the top three. The fourth is a booming business — private lending (17.1%). An interesting sidebar from the data was that "…at one point, one in $10.00 CAD used to purchase a condo in the Greater Toronto Area was from a private lending source."

In Canada, private mortgages are **not** subject to anti-money laundering rules. The unregulated lender is not required to identify the person beyond their own policies to avoid losing money. That typically involves just making sure they have enough equity to cover any losses in the event of a default. Some lenders are better than others but strictly due to their own policies — not regulation.

Legislative Update: Third Party Determination

There Has Been A Change!

Based on FINTRAC's updated guidance on 'Third party determination requirements', effective June 1, 2021, I seek clarification, particularly with respect to the exception of a cash deposit by an employee.

Specifically, in the archived version of the guidance directives, it stated:

"When a person is acting on behalf of their employer, the employer is considered to be a third party, except when the person is making a cash deposit into the employer's business account."

Now, the Regulations and Section 7 or its equivalent is absent from the current version of the Regulations. In other words, as of midnight June 1st, 2021, it seems they are now acting on behalf of a third party, while at 11:59 on May 31st, 2021 they were not.

1. Is this exception, as noted above, still applicable or not (where employee makes cash deposit as instructed by the employer)?

This exception is no longer applicable. Section 7 of the PCMLTFA was repealed (as of June 1, 2021), giving reporting entities greater flexibility when making a third party determination and when completing the ***on behalf of*** *section of a report. Reporting entities must now determine whether the employer is instructing the transaction or if there is another instructing party to consider.*

2. If the cash depositor is a beneficial owner of the entity and not the employee, would a third party determination situation still arise?

Yes. Each transaction's third party determination must be made on a case by case basis to capture any true third party.

FINTRAC Interpretation (ABCsolutions, September 2021)

FATF Report:

Ethnically or Racially Motivated Terrorism Financing

Ethnically or racially motivated terrorism (EoRMT) is a complex phenomenon that encompasses a wide range of actors. These range from individuals that operate as lone actors or so called "lone wolves" to small and medium organizations, as well as transnational movements that span borders and sometimes even continents.

This FATF report found that extreme right wing terrorist (ERWT) attacks are mainly perpetrated by self-funded lone actors, and extreme right wing (ERW) groups employ an array of fundraising techniques. These include:

- donations (through both crowdfunding and private contributions),
- membership fees,
- commercial activities (including organization of concerts, sales of merchandise, and real estate ventures), and
- criminal activities.

Notably, most of the funding for ERW groups appears to come from licit sources. ERW groups appear to be less concerned with concealing their transactions than in other forms of terrorist financing (TF), also ERW actors are becoming increasing operationally sophisticated in how they move their funds.

A dual outcome: The COVID-19 lockdown restrictions on mass gatherings throughout 2020 and 2021 have significantly affected an important financial source for ERW groups, namely the cancellation of ERW concerts and events. At the same time, the COVID-19 crisis has provided a recruitment opportunity for violent extremist groups. This may mean that ERW groups may seek new methods of funding or to an increased use of already existing sources.

This is the first in a series of two articles. This article looks at the sources of funds: donations; membership fees; commercial activities; criminal activities and the abuse of non-profit organizations. The next article will look at the movement of funds and the use of funds.

Sources of Funding

Donations – Crowdfunding is the practice of soliciting contributions from a large number of people, especially from the online community, usually in smaller amounts, to support an idea or a project. Crowdfunding and online commerce allow ERW groups to collect funds in a perfectly legal way. One of the factors underlying such prominence of crowdfunding is a generally high level of online activity of many ERW groups in social media, forums, gaming chatrooms, and other internet platforms. Reliance on crowdfunding models also allows ERW groups to collect funds from across a larger audience that shares ERW ideology, going beyond the local community or country.

Canada: In June 2019, Canada designated two Ideologically Motivated Violent Extremists (IMVE) as a means of disrupting their fund-rising activities (Blood and Honour and Combat 18). Additionally in February and July 2021, Canada designated several new IMVE groups as terrorist entities (https://www.fintrac-canafe.gc.ca/intel/bulletins/imve-eng). Designating ERW actors as terrorist entities can be a powerful tool, preventing them from access to the international financial system and disrupting their public fundraising capabilities.

Private Donations are also one of the common methods for ERW groups to generate funds. Unlike crowd-

funding, where the financier often does not have trusted relationships with the vast majority of donors, private donations are often based on the personal contact between the donors and the recipient. For some ERW groups, individuals willing donate money first have to be vetted through communication via encrypted email with the group members.

Membership Fees are another common method of raising funds for ERW groups. Unlike crowdfunding and donations, both of which are forms of voluntary support often provided by persons external to the group, fees are collected from members and are mandatory to pay. This is similar to the practices used by organized criminal groups, where lower-level criminals must regularly pay dues to higher-level criminals. Some ERW groups collect membership fees in cash or by using bank accounts held at local or regional FIs.

Reliance on membership fees by ERW groups appears to be a different practice from the financial strategies applied by other terrorist organizations such as ISIL, Al-Qaeda, and their Affiliates. Many of such organizations have not collected membership fees, but instead, some of them pay salaries to their members. For example, ISIL has been known to pay its fighters in the conflict zone.

Commercial Activities - Similar to other groups united by ideology, ERW groups do not declare profit generation as their main objective. However, some ERW groups have been engaged into various commercial activities, such as organizing:

- music festivals and concerts, football matches, martial arts events,
- selling various merchandise goods, i.e., clothing, books, ERW symbols or group logos, and distributing memorabilia, and
- real estate related deals (owning real estate provide a legitimate address to create companies that can be further used for business purposes).

Apart from providing a steady income to the group, these activities also facilitate the promotion of the ERW ideology, creating the potential for future recruitment and building links between various ERW actors.

Criminal Activities - Building links with organized crime enables ERW groups to generate revenue. It also provides opportunities to get access to restricted or illicit goods, such as weapons or forged documents, which allows the groups to increase their criminal activities.

Abuse of Non-Profit Organizations (NPOs) - NPOs play a vital role in the world economy and in many national economies and social systems. They also provide important charitable services to vulnerable populations, including those in and near conflict zones. Various FATF reports have identified cases in which terrorists and terrorist organizations exploit some NPOs to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organizations and operations, and where terrorists create sham charities or engage in fraudulent fundraising for these purposes. However, not all NPOs are inherently high risk for TF (and some may represent little or no TF risk at all).

While examples of NPO abuse by ISIL and Al-Qaida have been identified, other terrorist groups have also sought to abuse NPOs, including ERW groups. For example, some jurisdictions have identified private foundations that are ideologically aligned with some ERW groups (but may not openly support violence). These foundations can provide indirect support to ERW recruitment by financing books or research that supports ERW ideology. In other instances, an NPO aligned with an ERW group (such as one having affiliated individuals in leadership positions in both groups) can offer legitimacy to the group by engaging in charitable activities (food drives or fundraising activity) among sympathetic populations. Additionally, some NPOs affiliated with ERW groups may offer paramilitary or survival training to identify ideologically aligned individuals and start their recruitment into a group.

The next in this series of articles will discuss the movement of funds: financial institutions; money and value transfer services; cash; virtual assets, and financial management and the use of funds.

Source:
https://www.moneylaunderingnews.com/wp-content/uploads/sites/12/2021/07/FATF-Ethnic-or-Race-Motivated-Terrorist-Financing-Report.pdf

Beyond Our Borders

Bolivia

Bolivia is a landlocked country located in western-central South America. It is bordered by Brazil to the north and east, Paraguay and Argentina to the south, Chile to the southwest, and Peru to the west.

Money Laundering & Terrorist Financing

According to the **International Narcotics Control Strategy Report (INCSR–2021),** Bolivia is listed as a *country of primary concern* for money laundering. Bolivia is not a regional financial centre but remains vulnerable to money laundering. Illicit financial activities are primarily related to the cocaine trade, smuggled goods, corruption, and informal currency exchanges.

There is a large market for smuggled goods in Bolivia, most of which arrive by way of Chile. There is no indication the illicit financial activity is linked to terrorism financing; although a lack of proper safeguards leaves the economy vulnerable to such activity.

Bolivia has thirteen free trade zones for commercial and industrial use. Casinos are generally illegal in Bolivia, as are informal exchange houses and non-registered currency exchanges.

Bolivia takes a *list* approach to defining predicate crimes for money laundering. Enhanced due diligence procedures are required for both domestic and foreign politically exposed persons. Banks, micro-financial institutions, insurance companies, exchange houses, remittance companies, securities brokers, money transport companies, and financial intermediaries are all subject to Know Your Customer and suspicious transaction reporting requirements.

A few legal casinos pay a hefty percentage to the government in order to run card games, roulette, slots, and bingo. Many illegal casinos operate in the informal market.

Bolivia is a member of the Financial Action Task Force in South America (GAFISUD), a FATF-style regional body. Its financial intelligence unit, the Unidad de Investigaciones Financieras, is a member of the Egmont Group of Financial Intelligence Units.

Bolivia passed several laws to control the entry and exit of foreign exchange and criminalize illicit gains. The National Council to Combat Illicit Laundering of Profits issues guidelines and policies to combat money laundering. Regulatory procedures allow for freezing and confiscation of funds and other assets related to money laundering. All financial institutions in Bolivia are required by the Financial Investigative Unit (UIF), Bolivia's FIU, and banking regulations to report all transactions above $3,000 ($10,000 for banks).

Drug Flow / Transit:

Bolivia is one of the world's three largest cocaine producers and a significant transit zone for Peruvian cocaine. Most Bolivian cocaine flows to other Latin American countries, especially Brazil, for domestic consumption or onward transit to West Africa and Europe. In September 2020, the United States determined that Bolivia failed demonstrably to adhere to its obligations under international drug control agreements and the U.S. *Foreign Assistance Act of 1961*, as amended. This determination was based, in part, on the Bolivian government not taking sufficient measures to safeguard the country's licit coca market from criminal exploitation.

Corruption

The Bolivian justice system is hindered by corruption, political interference, and a lack of interagency cooperation, which impede the fight against narcotics-related money laundering. The lack of well-trained prosecutors and police officers has also been a problem, leading to ineffective criminal investigations. In 2017, the attorney general created a special unit dedicated to investigating and prosecuting money laundering.

(Continued on page 15)

Case Studies

Use of IP address associated with Darknet Marketplace – Alpha Bay

AlphaBay, the largest criminal darknet market dismantled by authorities in 2017, was used by hundreds of thousands of people to buy and sell illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals over a two-year span.

The site operated as a hidden service on the TOR network to conceal the locations of its underlying servers as well as the identities of its administrators, moderators, and users. AlphaBay vendors used a number of different types of Virtual Assets (VA), and had approximately 200 000 users, 40 000 vendors, 250 000 listings and facilitated more than USD 1 billion in VA transactions between 2015 and 2017.

In July 2017, the U.S. Government, with assistance from foreign counterparts, took down the servers hosting the AlphaBay marketplace, arrested the administrator, and pursuant to a seizure warrant issued in the Eastern District of California, seized the physical and virtual assets from the marketplace itself, and those that represented the unlawful proceeds from the AlphaBay criminal enterprise. Federal agents obtained the warrants after tracing VAs transactions originating from AlphaBay to other VA accounts and identifying bank accounts and other tangible assets controlled by the alleged administrator.

Customer profile does not match with regular high-value Virtual Asset trading

A Virtual Asset Service Provider (exchanger) and an FI (payment institute) filed STRs with the FIU concerning a high value of VA trading that began when the account at the exchanger was opened. Specifically, the account holder had been carrying out various VA buying and selling transactions for over EUR 180,000, which did not match the profile of the account holder (including occupation and salary).

Analysis found that the VAs were subsequently used for:
(i) transactions on a darknet market; (ii) online betting; (iii) transactions with VASPs that did not have adequate AML/CFT controls or that were under previous ML investigations involving millions of dollars; (iv) operations on platforms that offered peer-to-peer transactions of VAs; and (v) "mixing". The account holder had also made use of a variety of different means (e.g. money transfer, online banking, and prepaid cards) to move a consistent amount of funds out of his account in the same time frame.

The funds received by the account holder appeared to come from a network of individuals who bought VAs (Bitcoin) in cash and were located in different jurisdictions in Asia and Europe (including Italy), both via money transfer and the banking system. He also received funds on his prepaid cards from subjects in Africa and the Middle East, who in turn collected funds from fellow citizens residing in Italy and abroad. These funds were then used for cross-border transfers and online gambling, and were withdrawn in cash from ATMs in Italy.

Source: FATF (September 2020)
http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

Typologies Report: Evasion of Sanctions September 2021

Asia/Pacific Group on Money Laundering

The Asia/Pacific Group on Money Laundering (APG) produces regional typologies reports on money laundering (ML) and terrorist financing (TF) techniques in the Asia/Pacific region; Canada is a member of this group.

Obligations aimed at countering the financing of proliferation of weapons of mass destruction (WMD) under the FATF R.7 focus on jurisdictions' implementation of two jurisdiction-specific regimes created by United Nations Security Council Resolutions (UNSCRs): the Democratic People's Republic of Korea (DPRK) and Iran. Broadly, R.7 requires jurisdictions to freeze, without delay, the funds or other assets of, and ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of (a) any person or entity designated by the United Nations Security Council (UNSC), (b) persons and entities acting on their behalf or at their directions and/or (c) those owned or controlled by them.

The use of cryptocurrency to evade sanctions and raise revenue is a feature of modern day proliferation financing (PF). In 2019, RUSI (Royal United Services Institute) published a landmark study on DPRK's cryptocurrency activities in Southeast Asia. This study set out the various steps in PF where cryptocurrencies can be abused:

- **Acquisition:** Cybercrime is unquestionably the most prevalent method of sanctioned actors obtaining cryptocurrencies, especially by hacking cryptocurrency exchanges in East Asia. DPRK has also been involved in ransomware campaigns, such as 'WannaCry', and has been particularly interested in phishing and online fraud in the last few years.
- **Movement typologies:** Like traditional money laundering, large-scale cryptocurrency launderers such as DPRK use layering as a technique. Attackers create thousands of transactions in real time through one-time use cryptocurrency wallets. They are then able to muddy their tracks and break the transaction path.
- **Exchanges:** It has become increasingly clear that DPRK relies heavily on unregulated or noncompliant exchanges to launder funds, as well as peer-to-peer exchanges. Lack of regulation in many jurisdictions makes this pursuit relatively easy.
- **Liquidation speed:** DPRK generally cashes their cryptocurrency into fiat currency or another cryptocurrency relatively quickly, with liquidation speed increasing recently. There appears to be little interest in stockpiling cryptocurrency for future use.
- **Scale:** According to the most recent analysis, DPRK hackers are estimated to have stolen at least $1.75 billion from cryptocurrency exchanges.

The reports also flag the continued exploitation of the shipping industry through ship-to-ship transfers, laundering of ship identification, manipulating flags and vessel identifiers, and technological methods of deceiving automatic identification system tracks.

RUSI's Project Sandstone uses open source data-mining and data-fusion techniques to spot DPRK sanction evasion activities, particularly in the maritime space. The project aims to provide open-source intelligence and actionable evidence to those engaged in enforcement and the policy community in general. Investigations in Project Sandstone include research into DPRK's oil procurement networks, typologies for the movement of DPRK funds through the international finance system, and the significance of the city of Dandong in trading companies associated with PF.

(Continued from page 13)

On Transparency International's **Corruption Perceptions Index 2020**, Bolivia is ranked at 124/180 countries and territories surveyed, with a score of 31/100 on an index scale of 0 (highly corrupt) to 100 (very clean) compared to Canada, which is ranked at 11/180 with a score of 77/100.

Next Steps:

Bolivia should continue its implementation of its laws and regulations with the goal of identifying criminal activity that results in investigations, criminal prosecutions, and convictions.