Issue I

FIU-Nepal Newsletter

October, 2021

Inside this issue

Contact

Central Office
Baluwatar, Kathmandu

Tel: 01-4410201 (Ext. 841 / 418)
Fax: 01-4441051
Email: fiu@nrb.org.np
Website: http://www.nrb.org.np/departments/fiu

Director's Note

This is the second year in a row; the world has been fighting against the challenges of the Covid-19 pandemic. Once again, we have passed through frequent lockdowns, closures, restrictions in travel and movements due to the pandemic. As usual, the FIU-Nepal remained committed and dedicated to perform its functions mandated by the Assets (Money) Laundering Prevention Act 2008, Rules 2016 and FIU Bylaws 2020 even in an adverse scenario. Looking back over the past twelve months, we have reasons to be happy for the FIU-Nepal and indeed all the stakeholders have managed to get done amidst this uncertain environment.

FIU-Nepal has a core function of dissemination of financial intelligence relating to AML/CFT to the domestic law enforcement agencies. In addition to our core function of Analysis, we have legal mandate to coordinate with domestic and international agencies. We are in close coordination with the Reporting Entities (REs), Regulators, Law Enforcement Agencies (LEAs) and Prosecutors on AML/CFT issues.

FIU-Nepal has implemented goAML System for receipt, analysis and dissemination of suspicious activities and transaction reports. Commercial banks, Development banks and Finance companies are already integrated into the full-fledged production environment so far. FIU-Nepal is also working with other reporting entities to integrate in the goAML system gradually.

Nepal has formulated and implemented AML/CFT National Strategy and Action Plan (2019-2024). We are in close coordination with the various agencies for the implementation of the action plan. In the past, we worked with various agencies to complete AML/CFT National Risk Assessment (NRA) 2020. Now, we are working with various agencies for the preparation of upcoming Mutual Evaluation. Moreover, we have been coordinating with foreign FIUs for the exchange of information.

I take this opportunity to thank Nepal Rastra Bank, all the domestic stakeholders including reporting entities, regulators, LEAs, National Coordination Committee (NCC) and other committees/mechanisms for their continued support and cooperation. I would also like to thank Asia Pacific Group (APG) secretariat, EGMONT group and our foreign counterparts for their continuous support to FIU-Nepal.

Finally, I would like to thank all the employees of FIU-Nepal, who worked with dedication to make it possible for most of the progress made during this period. I hope this newsletter will be useful to get acquainted with activities of FIU-Nepal.

We welcome comments and suggestions for future improvements.

Dirgha Bahadur Rawal
Head/Director, FIU-Nepal

National Risk Assessment, 2020

Understanding the money laundering and terrorist financing risks is an essential part of national anti-money laundering/countering the financing of terrorism (AML/CFT) regime. A risk assessment allows countries to identify, assess and understand its money laundering and terrorist financing risks. Once these risks are properly understood, countries can apply AML/CFT measures that correspond to the level of risk, in other words: the risk-based approach (RBA). The risk-based approach, which is central to the FATF Recommendations, enables countries to prioritise their resources and allocate them efficiently. The FATF has developed guidance which will assist countries in the conduct of risk assessment at the country or national level (FATF Recommendation, 2013).

As per the updated FATF recommendations, each country has to conduct National Risk Assessment (NRA) to identify threats and vulnerabilities in its AML/CFT system that would inform the design of a policy framework and its implementation strategy including the resource prioritization. The Self Evaluation report (2018) has assessed the country's AML/CFT system based on the 40 recommendations. The gaps on country's AML/CFT system are explored and recommendations are made. Moreover, rating is done against each criterion of the FATF recommendations.

One major objective of National Strategy and Action Plan relating to money laundering and terrorism financing (2019-2024) is to conduct the NRA. Nepal has conducted the second National Risk Assessment in 2020. The outcomes of the NRA have provided guidance for the regulators, LEAs and other competent authorities to direct their efforts towards riskier areas. It has identified the major risk areas of ML/FT.

The major identification of the National Risk Assessment Report, 2020 is summarized as below:

- Significant achievements have been made in strengthening the legislative, regulatory and enforcement measures related to AML/CFT regime. Establishment of necessary institutions such as DMLI, FIU; formulation and enactment of a number of laws, delegated legislations and regulatory manuals; designation of 11 agencies as regulators are some of the key examples.
- In the international front, Nepal has ratified various international conventions and instruments related to AML/CFT and also become a member of AML/CFT related international institutions such as APG, Egmont group of FIUs, ARIN-AP.
- There is lack of proper understanding on issues of AML/CFT across the public and private sectors; especially on the issue of KYC and electronic KYC.

The Report has identified following threats:

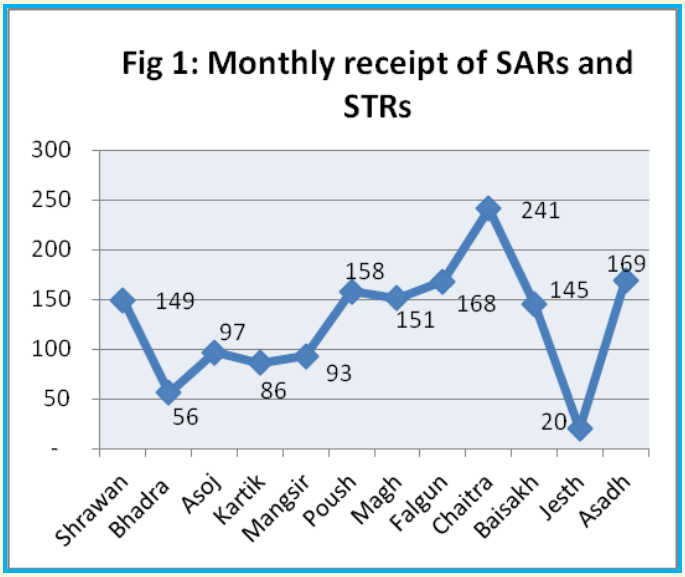
- **Major threats:** Corruption (bribery), tax (revenue) evasion, financial crimes such as banking offence and hundi.
- **Threats of concerns:** Drug trafficking, organized crime, extortion, arms-related offence, domestic terrorism, fraud, counterfeiting of currency, environment related crime, robbery (theft), smuggling (including black marketing) and forgery.
- **Low threats:** counterfeiting and piracy of products, kidnapping, illegal restraint and hostage taking, international terrorism, trafficking in stolen goods and insider trading.

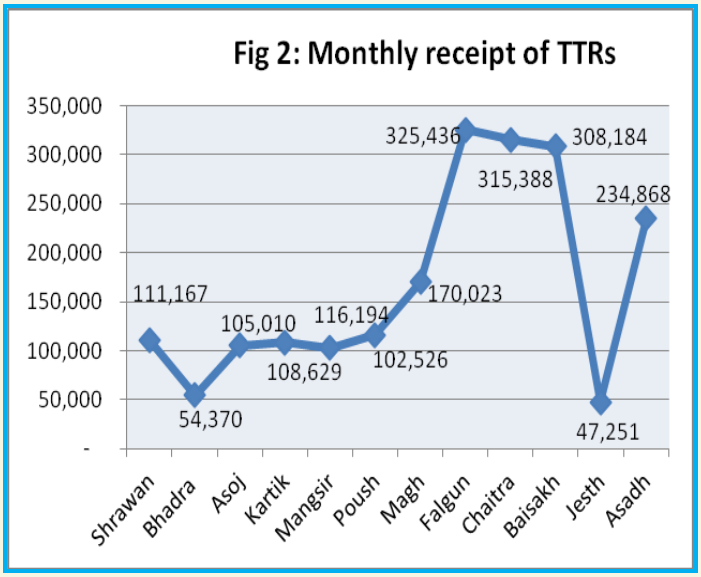
- The existing AML/CFT legal, policy and institutional frameworks provide relatively comprehensive provisions in line with the standards and good practices of FATF such as CDD, monitoring, reporting, record keeping, regulation, supervision, prohibition of fictitious and anonymous accounts & transaction with shell banking, monitoring PEPs, wire transfer, non-face-to-face technology based financial activities.
- However, there are a few designated predicate offences/conducts that are yet to be criminalized including categorical criminalization of terrorism. There are limitations in the laws on business regulation of casinos, real estates and collection of beneficial ownership information.
- Banking sector is reporting STRs in acceptable numbers whereas reporting from other sector is limited.
- There is functional overlapping of DMLI and other LEAs, including the lack of sharing information and organization of parallel or joint financial investigation on the basis of risks.
- **National vulnerabilities** assessment across the sectors found weaknesses related to effective supervision of REs, robustly continuing the recent tax reform initiatives, tightening the domestic and international trade discrepancies including the issues of remittance and hundi.
- The overall **banking sector** vulnerability to ML is rated as medium-high whereas; the quality of the general AML control is medium. Large business-related credit products are found to be highly vulnerable products with medium-high rating, current deposit product is rated as medium-high and natural persons saving accounts are rated medium.
- The overall **cooperative sector**'s vulnerability to ML is rated as medium-high due to the implementation issues of the existing AML/CFT laws.
- The overall **securities and insurance sector's** vulnerability to ML is rated as medium.
- Though money changers and remittance companies are licensed and regulated, informal remittance or value transfer services or ***hundi*** dealers pose serious challenges and is assessed as an area of high concern.
- Among **DNFBPs, 'casinos'** and **'dealers in precious metals and stones'** operate with minimum business regulation and are often unaware of their AML/CFT obligations, thus their vulnerability has been assessed medium-high. The **real estate sector** is most vulnerable to ML and rated high due to lack of business laws regulating them for licensed business. **Independent legal, notary and accounting professionals** are assessed as medium level vulnerability.
- Lack of laws requiring the AML/CFT measures and national statistics related to the **Non-Profit making Organizations (NPOs)** are the main problems, so, the vulnerability of this sector is assessed as medium.
- The assessment report has made a number of recommendations on the basis of its findings. These findings and recommendations are identified and incorporated in the National AML/CFT strategy and Action plan 2019-2024.

Activities in Numbers

FIU-Nepal is responsible for receiving, processing, analyzing and disseminating financial information and intelligence on suspected money laundering and terrorist financing activities to the relevant law enforcement agencies and foreign FIUs. As specified in the ALPA 2008, it disseminates information about suspected money laundering or terrorism financing or predicate offence to LEAs as per their scope and jurisdiction. Dissemination involves the disclosure of sensitive, personal, financial and law enforcement information, and measures need to be applied to ensure that the information is properly protected, that disclosures are documented, and that dissemination is made to the appropriate authorized recipient.

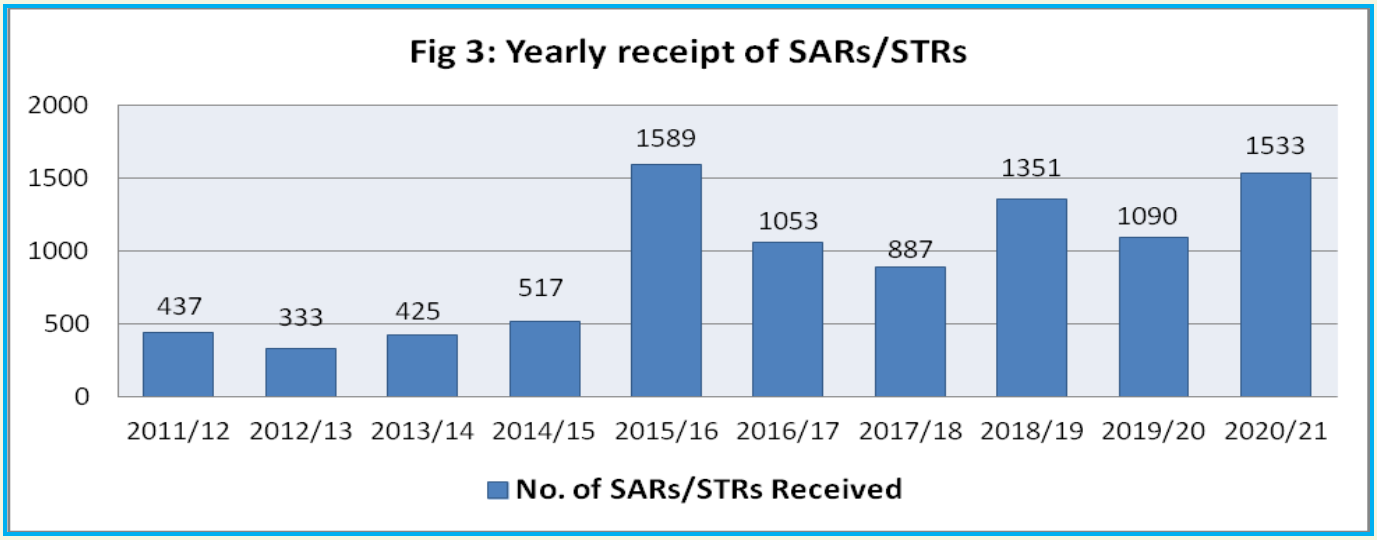
Monthly receipt of SARs/ STRs and TTRs (FY 2020/21)



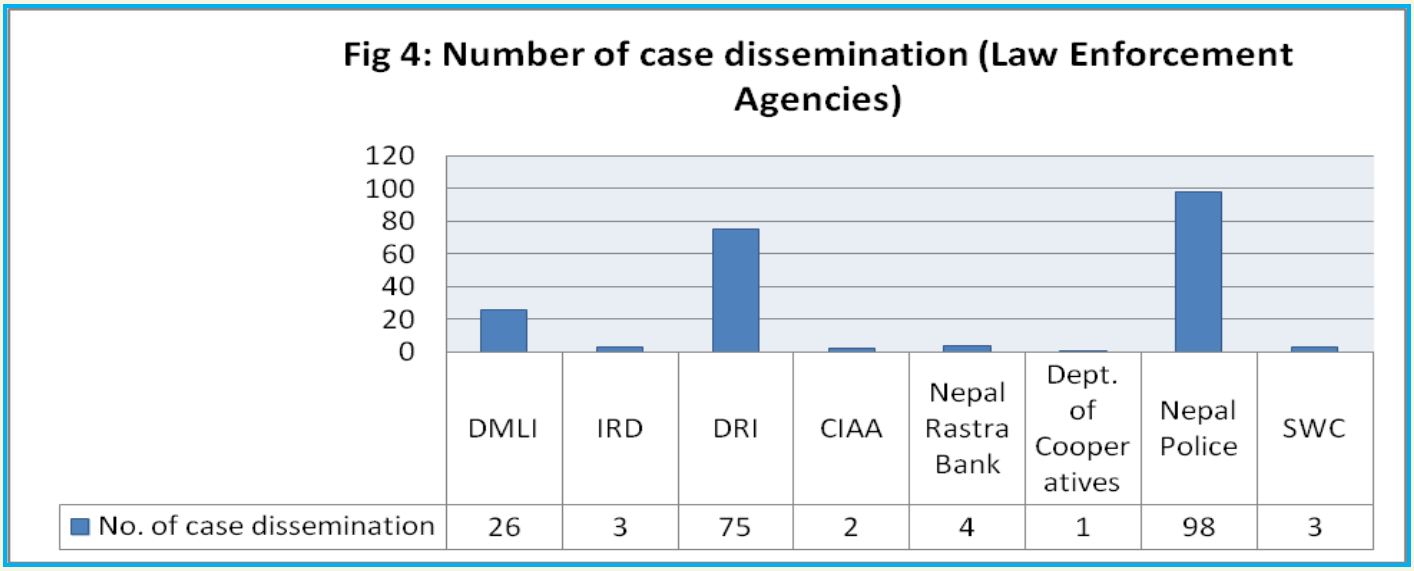


**Monthly data are presented as per the Nepali Calendar (Fiscal Year-mid July, 2020 to mid July, 2021)*

Yearly receipt of SARs/STRs



Agency wise dissemination of SARs/STRs (FY 2020/21)

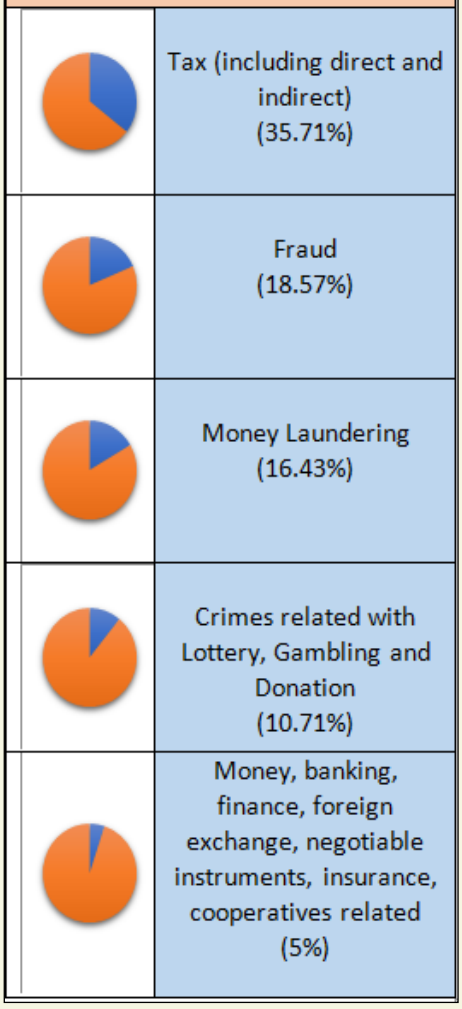


Predicate offence-wise case dissemination (FY 2020/21)

S.N.	Predicate offence	Number
1	Any kinds of sexual exploitation including the sexual exploitation of children	2
2	Crimes related with Lottery, Gambling, Donation	15
4	Fraud	26
5	Forgery	4
6	Tax (including direct and indirect)	50
7	Money, banking, finance, foreign exchange, negotiable instruments, insurance, cooperatives related	7
9	Smuggling (including custom, excise and revenue)	2
10	Trafficking in person and migrant smuggling	3
11	Extortion	1
12	Corruption and bribery	1
13	Money Laundering*	23
12	Real estate and property	6
Total		**140**

** Money laundering is not classified as predicate offence in ALPA, 2008. It is included here as a type of offence.*

Top five predicate offences related to case dissemination



Implementation of goAML

The goAML application is a fully integrated software solution developed specifically for use by Financial Intelligence Units (FIUs) and is one of UNODC's strategic responses to financial crime, including money-laundering and terrorist financing.

FIU-Nepal is actively involved in the implementation of goAML Software in reporting entities. During the implementation of goAML, various issues of different reporting entities has been addressed by customizing the goAML software to meet the data requirements of them. Currently, banks and financial institutions (class A, B and C), insurance companies, remittance companies, securities companies, few co-operatives are registered in goAML. FIU-Nepal is working to integrate Microfinance companies, payment service providers/operators (PSPs/PSOs), DNFBPs, EPF, CIT, etc. so that it can embrace all the financial sectors of the country and have complete database in goAML system.

In the process of incorporating different reporting entities like remittance companies, life and non-life insurance companies, securities companies, cooperatives in goAML, FIU-Nepal has organized various programs and has provided the test login for reporting in goAML test environment.

FIU-Nepal regularly organizes different interaction programs/ seminars/workshop with REs for the effective implementation of goAML. In this year, it has conducted various interaction programs with REs both physically and through online platform despite the adverse impact of covid-19 pandemic.

Reporting entities statistics in goAML

Reporting Entity Type	Test Environment	Production Environment
Class A	27	27
Class B	19	19
Finance Company	18	18
Insurance Company (Life and Non-Life)	40	0
Security (Stock Broker, Stock Exchange, Merchant Banker)	84	0
Remittance Company	16	0

The goAML software is upgraded recently from version 4.6.0 to 4.8.0. In this version we can customize our system as per the need and requirements. The enhanced security feature of goAML will be helpful to protect data from tapping or security related issues. The data fields are available so that we can make proper template for different process of analysis. The goAML implementation process will be continued until we incorporate all the reporting entities and LEAs in goAML system.

Photo: Interaction program with Insurance Companies

Mutual Evaluation of Nepal

In accordance with APG membership rules, on joining the APG, members commit to a mutual peer review system to determine the levels of compliance with the international AML/CFT standards. These peer reviews are referred to as "mutual evaluations".

Mutual Evaluation of Nepal is carried by Asia/Pacific Group on Money Laundering (APG) as Nepal is one of the members of this group. The evaluation is usually carried through onsite inspection by the special team of experts who makes a detailed analysis of each country's system on the basis of relevant AML/CFT rules and regulation, guidelines and other institutional framework for preventing criminal abuse of the financial system. The basic objective of the mutual evaluation is to assess the legal and institutional compliance level and the extent to which the defined outcomes are achieved.

Nepal was evaluated for the first time in 2005 based on FATF 40 plus 9 standards. Nepal was rated Non-Compliant (NC) on 34 recommendations, Partially Compliant (PC) on 8 recommendations, Largely Compliant (LC) on 4 Recommendations and 3 recommendations were Non-Applicable (NA). It was before promulgation of Assets (Money) Laundering Prevention Act hence, money laundering offence was not criminalized. The Act was later enacted in 2008.

Nepal was evaluated for the second time in 2010 against the FATF previous 40 plus 9 standards. The report was adopted in July 2011 where Nepal was rated NC or PC on 43 recommendations, LC on 3 recommendations, NA on 2 recommendation and compliant on one recommendation. Out of the 16 core/key recommendations Nepal was NC or PC on 15 Recommendations and LC on one recommendation. Department of Money Laundering Investigation was institutionalized later

in 2011. However, Nepal's progress after the evaluation was so substantial that it had technically (legal and institutional) resulted LC in 10 Core/Key Recommendations. These achievements have also assisted Nepal to come out from the APG Expedited/Enhanced as well as from regular monitoring in 2014. As a result, Nepal came out from the Grey list in 2014, as FATF announced "significant progress in improving the AML/CFT regime".

The third mutual evaluation will be assessed in the effectiveness for visible implementation and outcomes in addition to technical outputs and laws. Also, APG has published APG Third Round of Mutual Evaluation Procedures-supplementary procedures during the period of COVID-19 global pandemic in February, 2021.

The mutual evaluation is based upon FATF Methodology 2013 for assessing compliance with FATF recommendations and the effectiveness of AML/CFT System. Mutual Evaluations have four basic components i.e., Risk and Context, Technical Compliance Assessment, Effectiveness Assessment and Integrated Conclusions and Recommended Actions.

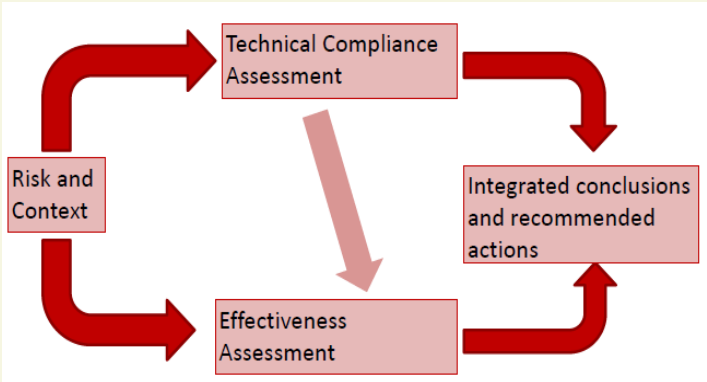


Fig 5: Mutual Evaluation Process

The APG members' follow-up reporting deadline ('streams') for Nepal has been scheduled for 2023-25* under APG Third Round Mutual Evaluation Procedures revised in July, 2021 (commencing 2024 if COVID-19 pandemic restrictions continue). Currently, various committees have been formed to facilitate and prepare for the mutual evaluation of Nepal. These committees are working even during the covid-19 pandemic to submit reports, data and other requirements of the assessor team.

Memorandum of Understanding (MOU) with Domestic Agencies

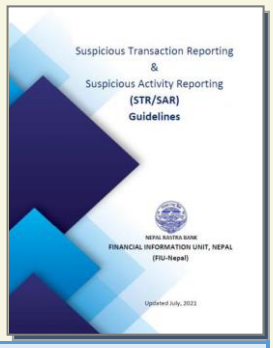
On 23 January 2021, FIU-Nepal has signed MOU with Department of Customs. Mr. Suman Dahal, Director General, Department of Customs and Mr. Dirgha Bahadur Rawal, Head/Director of FIU-Nepal signed the MOU on behalf of two institutions.

Money launderers and terrorist financiers are most often internationally connected and operate across borders. Department of Customs need to share suspicious Cash and BNIs movement to FIU-Nepal. Therefore, the MOU will facilitate greater co-operation and co-ordination between the two institutions in the exchange of information relating to the money laundering and terrorist financing.

The MOU entered with Department of Customs is the third of such MOU entered with domestic agencies. Previously, FIU-Nepal has already signed MOU with Department of Money Laundering Investigation and Nepal Police-Central Investigation Bureau on 3 December, 2013. Arrangements are currently being made to sign similar MOUs with other domestic agencies to facilitate the exchange of information thereby mutually benefiting the Nepal's effort in combating Money Laundering and Terrorist Finncing.

Photo: Signing of MOU with Department of Customs

Updated "*Suspicious Transaction and Suspicious Activity Reporting (STR/SAR) Guidelines*"



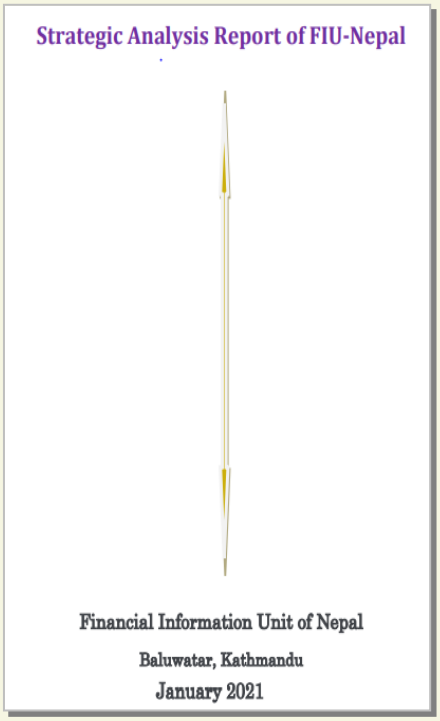
FIU Nepal recently updated and published its STR/SAR Guidelines. The major updates of the guidelines are:

- ✓ REs to assess risk while reporting STRs/SARs to FIU-Nepal based on threats identified and rated by National Risk Assessment Report, 2020.
- ✓ REs to provide a reference to the 'Predicate offence' listed in the ALPA, 2008 and where any particular offence(s) cannot be established then report should mention 'Money Laundering' as an offence while reporting STR/SAR.
- ✓ Reporting through goAML software should be as per 'goAML Operational Guidelines' and reporting instructions for REs, issued by FIU-Nepal.
- ✓ Red flags for Cooperatives, PSPs and PSOs sectors have been added. In addition, new indicators for STR/SAR have been incorporated.
- ✓ It also includes potential ML/TF risks emerging from COVID-19 and post-pandemic environment such as increased misuse of online financial services and virtual assets to move and conceal illicit funds; misuse and misappropriation of domestic and international financial aid, frauds related to medical products, exploitation of money mule schemes, etc.

Updated guideline is expected to improve the quality of STR/SAR, identify predicate offence(s) and adopt the risk based approach by REs in assessing the quality of AML risk.

Strategic Analysis Report

Strategic analysis uses available and obtainable information, including data that may be provided by other competent authorities, to identify money laundering and terrorist financing related trends and patterns.



FIU-Nepal has started and continued to undertake strategic analysis of financial information gathered from reporting entities to enable FIU-Nepal and its stakeholders to understand the patterns and trends of money laundering and related issues. The strategic analysis has also enabled FIU-Nepal to draw conclusions for the strategic prevention of money laundering and financing of terrorism and for setting operational priorities. The Policy & Planning Division (PPD) of FIU-Nepal has published its first strategic analysis report in January, 2021. It also includes the data analysis of the various reports received at FIU-Nepal, its graphical representation, interpretations and various case studies.

The strategic analysis report was concluded with following general observations:

- Out of the two broad categories of the Reporting Entities; financial institutions are the main reporting entities while DNFBPs are in a nascent stage of reporting. Among the financial institutions, BFIs cover more than 90% of the STR/TTR reporting
- Tax evasion is the highest number of STR disseminations based on the classification of Typology
- Corruption (bribery), tax (revenue) evasion, financial crimes such as banking offence and hundi are the predicate offences which are classified as high risk (NRA 2020)
- FIU-Nepal is gradually integrating the reporting entities into the goAML system
- Awareness regarding AML-CFT needs to be enhanced in order to identify, assess and monitor the ML/TF risks in Nepal
- Covid 19 has increased the need and importance of online transactions. As a result, the need for new dimensions of risk management has also been changed rapidly
- Other sources of risks are the size of informal economy, open and porous border, awareness regarding AML-CFT and the initial stage of development of AML-CFT regime
- Gradual integration of reporting entities into the FIU database will contribute towards the identification, assessment and management of the ML/TF risk in Nepalese context.

Capacity Building

FIU-Nepal has made several strategic and operational efforts to enhance its capacity in FY 2020/21 for attaining its maximum degree of effectiveness. It has conducted numbers of training programs as well as coordinated with international agencies for their supports for training and workshops. In the first quarter of FY 2020/21, all FIU Staffs took two ACAMS online training courses on different topics related to AML/CFT. FIU-Nepal also conducted various knowledge sharing programs both virtually and physically.

FIU-Nepal had organized various interaction programs virtually and physically with different REs, regulators, LEAs and other agencies. On 14 December 2020, interaction program was organized virtually with LEAs on AML/CFT issues. It has also organized various interaction programs with insurance companies, securities companies, Citizen Investment Trust, Employee provident fund to discuss on AML/CFT issues and for the implementation of goAML. On 11 January 2021, FIU-Nepal organized virtual interaction program with DNFBPs and regulators to prepare them for reporting through goAML software. On 30 March 2020, in the presence of governor of Nepal Rastra Bank, it organized one-day interaction program on AML/CFT with regulators. It also organized interaction program virtually with compliance/IT officers of commercial banks, development banks & finance companies on 12 April, 2021 to discuss on the different issues on AML/CFT and effective implementation of goAML system. With the presence of all staffs, FIU-Nepal organized one-day knowledge sharing program on 15 July, 2021.

Photo: Interaction program with regulators

Photo: Knowledge Sharing Program

Impact of COVID-19 on ML/TF

On 30 January 2020, the WHO declared the outbreak of novel coronavirus constituted a public health emergency of international concern. Along with the human fatalities, it also invited serious problems through increased criminal opportunities arising from the misappropriation of government financial support payments, online banking fraud and misuse of online technologies among others. The majority of illicit activities associated with COVID-19 relates to proceeds generating offences such as financial fraud and exploitation scams, for example, criminals attempting to profit from the pandemic through fundraising for fraudulent charities.

COVID-19 pandemic has brought new and sizeable challenges for everyone around the world. It is impacting government and private sectors' abilities to implement AML/CFT obligations. Government and private sector employees are now working remotely; some are deployed to COVID-19 responses; or are not working at all. To some extent, especially for countries with more limited resources and less advanced business continuity planning, re-prioritization efforts by governments are likely to result in a reallocation of resources away from AML/CFT activities to other areas, such as financial stability, and humanitarian and economic recovery efforts. There have been indications that some countries with less resilient AML/CFT regimes or resources may be unable to maintain AML/CFT operations while they prioritize responding to COVID-19.

In May 2020 the FATF produced a paper entitled 'COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses' using information provided to the members of the FATF Global Network in April 2020 [FATF, 2020 (5)]. The paper identifies the potential money laundering and terrorist financing risks as:

- Criminals finding ways to bypass CDD measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds;
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
- Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds;
- As individuals move money out of the banking system due to financial instability, this may lead to an increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds;
- Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent money laundering risks;
- Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries, both for the laundering of proceeds as well as to fund their operations, as well as fraudulently claiming to be charities to raise funds online.

Cyber fraud prevention and security tips

Cybercrime covers a wide range of crimes, such as privacy leaks, harassment and cyberbullying, child exploitation and pornography. Additionally, scammers commit online fraud to gain illegal financial gain from another person through the use of internet technology.

According to a report released by the Federal Trade Commission (FTC), millennia are more likely to be victims of cyber predators, but people aged 70 and older lose more money through fraud. Of the 2.2 million fraud reports, a total of USD 3.4 billion was fraud losses. The number of online fraud cases in Nepal has also increased recently. The crackdown of more than hundreds of Chinese citizens, cases of lottery-based scams, Agricultural Development Bank hacking cases, and ATM hacking cases are just a few examples.

Scammers use sophisticated and advanced technology to attack their victims. Spoofing and phishing, corporate email compromises, and ransomware are common tools for an attacker to target a victim and steal their personal and financial information or demand a ransom. On the other hand, scammers use social engineering skills to lure victims to transfer money to their accounts.

Following tips help to minimize the threat of online fraud:

- Keep the firewall on your computer turned on to help you protect from the hacker who try to gain access to your system to steal your personal information or passwords.
- Install and timely update your antivirus software so that it can detect and remove the latest malicious codes and viruses that may have infected your system.
- Additionally, install antispyware and antimalware software to detect and remove malware and malicious code that collects information about you without your consent.

- Regularly update your operating system to receive the patches that fixes the security holes and vulnerabilities.
- Do not install software downloaded from untrusted and unknown source.
- Use a proper caution while plugging in removable devices such as USB received from events, exhibition or expo into office devices.
- Be careful what you click; like links on email, text messages, pop-ups and spam emails.
- Beware of the email that looks suspicious. Email that directs you to download the attachment from suspicious looking address may contain malware.
- Do not allow your web browser and websites to remember your password and credit card details.
- Do not give your password and One-time password (OTP) to anyone even if they claim to be from legitimate source.
- Use the strong passwords to your logins in social media accounts or online banking and if possible, use multi-factor authentication.

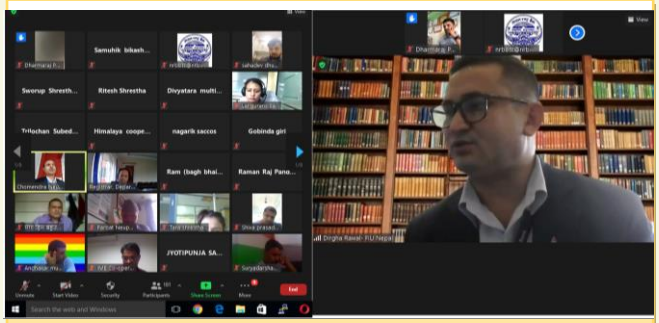
Not everyone will be a victim of cyber fraud, but they are still at risk. Cyber fraud is due to human weakness in evaluating actions that are safe or not from a cybersecurity perspective. Therefore, everyone has a duty to participate in the fight against cyber predators.

GALLERY

FIU-Nepal Team

Interaction program with Regulators

Interaction program with Nepal Police



Virtual interaction program with Cooperatives

Interaction program at NRB, Bhairahawa

Interaction program at NRB, Pokhara

Interaction program at NRB, Birgunj