Strategic Analysis Report, 2024

Cyber Enabled Frauds

Financial Intelligence Unit (FIU-Nepal)

Nepal Rastra Bank

Foreword

The Financial Intelligence Unit (FIU) Nepal serves as the national agency responsible for receiving, analyzing, and disseminating Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs), and Threshold Transaction Reports (TTRs). FIU-Nepal conducts operational and strategic analysis based on these reports. This fourth Strategic Analysis Report focuses on the trends and typologies of Cyber-Enabled Frauds (CEF) based on SAR/STR/TTR report received at FIU-Nepal.

After Covid-19 pandemic there is significant increase on reporting of CEF-related STRs/SARs at FIU-Nepal by commercial and development banks. The major findings of this report are, individuals aged 19-30 are predominantly involved in CEF and fraudsters commonly use multiple accounts opened in different Banks and Financial Institutions (BFIs) and Payment Service Providers (PSPs) under the same individual to collect illicit funds. The major sources of CEF-related STRs/SARs are victim reports and inquiries from law enforcement and investigative agencies.

This report is based on the analysis of STRs/SARs received, processed, and disseminated by FIU-Nepal. The report has recommendations for reporting entities, law enforcement agencies, and regulators/supervisors on minimizing CEF-related losses, drawing from both the analysis and international best practices. Additionally, the report highlights key red flags for reporting entities to detect CEF and summarizes some noteworthy practices adopted by various jurisdictions and organizations in combating CEF.

I extend my gratitude to everyone who contributed to the completion of this report. It is a collaborative effort of the Policy & Planning Division and the Analysis Desks of FIU-Nepal, with technical support from the goAML Implementation team. I also acknowledge the contributions and feedback provided by Prabhat Chhetri, Assistant Government Attorney, Office of the Attorney General, and Subash Hamal, Deputy Superintendent of Police (DSP), Nepal Police. I am especially thankful to Deputy Directors Keshab Prasad Rimal, Sworup Shrestha and Bishnu Prasad Guragain, and Assistant Director Kishor Mahara for their significant contributions on this report.

I sincerely hope this report will serve as a valuable resource for reporting entities, law enforcement agencies, regulators, supervisors, and the public.

Dirgha Bahadur Rawal

Director/Head of FIU-Nepal

Table of Contents

List of Tables

List of Figures

List of Abbreviations

Abbreviation	Definition
ALPA	Asset (Money) Laundering Prevention Act
AML	Anti-Money Laundering
APG	Asia Pacific Group
ATM	Automated Teller Machine
BEC	Business Email Compromise
BFI	Bank and Financial Institution
CDD	Customer Due Diligence
CEF	Cyber Enabled Fraud
CFT	Combating Financing of Terrorism
CIB	Central Investigation Bureau
CVV	Card Verification Value
DMLI	Department of Money Laundering Investigation
DRI	Department of Revenue Investigation
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GPS	Global Positioning System
INTERPOL	International Criminal Police Organization
IPS	Interbank Payment System
KYC	Know Your Customer
LEA	Law Enforcement Agency
MER	Mutual Evaluation Report
NRB	Nepal Rastra Bank
OTP	One Time Password
PSD	Payment Systems Department
PSP	Payment System Providers
REs	Reporting Entities
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UPI	Unified Payments Interface
VPN	Virtual Private Network

1. Introduction

1.1 Fraud

Fraud is a broad term, which involves wrongful or criminal deception in order to gain something unlawfully or unfairly. It is the crime of getting money by tricking or deceiving people. Fraud is an intentional distortion of the truth in order to induce someone to part with something of value or to surrender a legal right[1].

The term fraud has varied definitions and there are numerous types of fraud. In the study carried out by Asia Pacific Group on Money Laundering (APG), fraud has been broadly classified as (i) Robbery, (ii) Tax and excise evasion, (iii) False customs declaration, (iv) General fraud (Identity theft, Advance fee fraud, Lottery scams, Procurement fraud, Corporate fraud, Occupational fraud), (v) Financial instrument fraud (Cheque fraud, Credit card fraud), (vi) Internet/Technology enabled crime (Email spoofing, Dating fraud, Charity fraud, Money transfer fraud, Purchase fraud, Internet banking scam, Mass marketing fraud); and (v) Corruption and bribery (Embezzlement and misappropriation, Bribery)[2].

The APG report also mentions three major factors driving the fraud also known as fraud triangle.

- **Pressure:** It refers to a financial need. It is the catalyst that motivates an individual to commit fraud. It may arise from different reasons like gambling debt or maintaining lifestyle beyond ones means.
- **Opportunity:** It is the ability to actually commit a fraud. Opportunity increases with ease and lack of oversight. The easier to commit fraud, the more likely it is to occur.
- **Rationalization:** It is how an individual justifies committing fraud. Fraudsters often see themselves as victims of unusual circumstances and have to develop an explanation that make illegal behavior acceptable. It can range from helping oneself to helping others.

Fraud can occur both on a local and transnational scale. Individuals, corporates and even governments may be victim of fraud. Adoption of information technology in payment industry has further complicated the classification of fraud.

1.2 Cyber Enabled Fraud (CEF)

Cyber enabled fraud (hereafter referred as CEF) is a crime done using a computer with an intention of acquiring another person's personal and financial information that is stored online. It is the fraud enabled through or conducted in the cyber environment. Rise of digital payment after COVID-19 pandemic generated opportunity for fraudsters to commit fraud by exploiting digital payment systems and human vulnerabilities. Incidents of fraud have also become more organized and sophisticated like targeted hacking into networks and databases, phishing attacks etc.

Both individuals and organizations are prone to cyber-enabled fraud. The report published by Association for Financial Professionals (2022) suggested payments fraud activity is decreasing in case of organizations[3]. It had been increasing steadily since 2013 and in 2018 it reached peak. More than 81 percent of financial professionals reported that fraudsters targeted their organizations in

[1] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/fraud.
[2] APG Typologies Report on Fraud & Money Laundering in the Pacific, 2016
[3] Association for Financial Professionals (2022), Payments Fraud and Control Report, Underwritten by J.P. Morgan www.AFPonline.org

2019. Since then fraud has declined. In 2022 over 70% of companies continue to be targeted by fraudsters. Report found remote working did not play significant role in incidence of payments fraud in 2021. The share of organizations that were impacted by email fraud were also declined due to extensive efforts made by business leaders to safeguard employees vulnerable in remote working environment, training and other validation and verification processes. While there was decline in check fraud due to decrease in organizations using check in business to business transactions, incidence of fraud via Automated Clearing House (ACH) debit and credit was on rise. This finding was evidence that fraudsters are constantly innovating and devising plans to defraud organizations.

According to the INTERPOL Global Crime Trend Summary Report 2022[4], ransomware, phishing, online scams, and computer intrusion (i.e. hacking) are the cybercrime trends which member countries most frequently perceive as posing 'high' or 'very high' threats globally. As rate of digitalization have rapidly accelerated, particularly during the pandemic, online social engineering for the purpose of financial fraud, victim manipulation and impersonation frauds are increasing significantly. In Asia and Pacific region, ransomware, phishing, online scams, computer intrusion, and Business Email Compromise (BEC) were among the top ten crime trends most frequently perceived to represent a 'high' or 'very high' threat by member countries. INTERPOL's 2023 Global Crime Report too has identified Cybercrime as one of the eight crime areas with notable growth in a year[5].

The Reserve Bank of India (RBI)'s Annual Report 2022-23 has suggested clear increase in the number and value of payment frauds in India[6]. As reported by financial institutions (FIs) the volume of frauds using cards and internet banking was 2,545 in 2020-21, 3,596 in 2021–22 and 6,559 in 2022–23. The value of fraudulent transactions in 2020-21, 2021–22 and 2022-23 was INR 1.19 billion, 1.55 billion and 2.76 billion respectively.

According to the report of PricewaterhouseCoopers (2022),[7] common fraud typologies in Indian context are (i) Identity theft/impersonation (ii) Phishing/vishing (iii) Web skimming (iv) By using QR code (v) Social engineering (vi) Account takeover (vii) Database breach (viii) Remote access assistance (ix) Botnet attack.

There is no universal classification of fraud related typologies. Realizing the need of universal classification of fraud in payment systems, a cross-industry work group led by The Federal Reserve developed a model called 'Fraud Classifier Model[8] on June 2020 to help organizations to classify fraud involving payment systems. It provides a set of tools and materials to help provide a consistent way to classify and better understand the magnitude of fraudulent activity including how it occurs across the payments industry. The model enables payments stakeholders to classify fraud in a simple and similar manner. It can be applied across an organization to help ensure greater internal

[4] See https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf

[5] See https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports INTERPOL's 2023 Global Crime Report

[6] See https://rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1377 Reserve Bank of India's (RBI) Annual Report 2022–23, page 155 Table VI.3: Frauds Cases - Area of Operations.

[7] See https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf Page 7-8 Combating fraud in the era of digital payments (pwc.in) (May 2022) PricewaterhouseCoopers Private Limited.

[8] See https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/fraudclassifier-model/ FraudClassifier Model - FedPayments Improvement The Federal Reserve, FedPayments Improvement (2024)

consistency in fraud classification, information that is more robust and better fraud tracking. The model classifies fraud independent of payment type, payment channel or other payment characteristics. However, data about the actual adoption of the model like this by industries is not available.

1.2.1 Key sources of detection of cyber enabled frauds

There are two primary sources of information for detection and investigation of CEF related money laundering: victim reporting and Suspicious Transactions Reports (STRs)/ Suspicious Activity Reports (SARs).

Victim reporting:

Victim reporting is an important source of information for both detecting and investigating fraud related proceeds. In certain fraud cases like BEC fraud and phishing, reporting is done quickly as victims discover the fraud relatively quickly. It is because the payment has not reached the intended counterparty and so the counter party asks for missed payment. In other cases, like investment fraud and romance fraud victims may realize they were defrauded only after certain time period.

Timely victim reporting is important for successful investigation of fraud and tracing and recovery of illicit proceeds. It enables enforcement agencies to act quickly which increases success of investigation. Victims may report suspected crimes to LEAs, including dedicated units that handle fraud reports like Cyber Bureau of Nepal Police. Victims may also notify their financial institutions and payments providers about suspected fraudulent transactions in their accounts. Victims have also approached grievance management system looked after by Financial Inclusion and Consumer Protection Division of Nepal Rastra Bank (NRB).

However, in cases where victims suffer negligible losses, fraud is less likely to be reported. Under reporting may also be observed due to victims' emotional factors like embarrassment or fear.

Some jurisdictions have created dedicated platforms for victims to report fraud, including online portals in order to increase victim reporting. In India, Citizen Financial Cyber Fraud Reporting and Management System[9] is established which provides dedicated helpline number for fraud reporting to financial cyber fraud victims. In United Kingdom, Action Fraud[10], a national report center for fraud and cybercrime, runs an online 24/7 live reporting portal for victims. The standardized data capturing of these platforms help analysis of fraudulent transactions reports, which is useful to identify criminal trends. These platforms are also useful to relay awareness for fraud prevention.

Suspicious Transactions Reports (STRs)/ Suspicious Activity Reports (SARs)

STR/SARs are important detection sources for CEF because of possibility of low victim reporting. Most of CEF-related STR/SARs are filed by the banking sector.

Strategic analysis papers on CEF developed by FIUs may also be useful for reporting of STR/SARs and CEF detection. These initiatives also enhance detection and prevention of CEF crime by frontline bank staffs of financial institutions. Timely analysis of CEF-related STRs is important because of quick

[9] See more at https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158 (Detail in mentioned in Annexure)
[10] See more at https://www.actionfraud.police.uk/

laundering of proceeds of such crime. For this Financial Intelligence Units (FIUs) can adopt prioritization system and focus on the higher-risk CEF-related STRs.

1.2.2 Characteristics of CEFs

Based on jurisdictions' experience across different regions, the study of FATF[11] found that 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 these 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, like in case of parcel fraud, perpetrator may pretend to be employee of a courier company and may ask for customs charge to release valuable goods);
- Online medium or platform (used for communication like luring victims into lottery or gift frauds. It is also be used for victims to transact on. e.g., in cases of online trading fraud displaying goods in Instagram at attractive pricing and not delivering goods after obtaining advance payment).

Although the increasing trend of CEF is known to all jurisdictions, LEAs, PSPs and relevant parties are lagging behind the fraudsters. A study by Clinton Mills (2017)[12] has listed out five main difficulties associated with fraud prevention, which are relevant in case of Nepal as well:

- **It is uncommon**: Despite the fact that fraud is happening every day, legitimate transaction still significantly outnumbers fraudulent transactions. Most organizations do not experience excessive amounts of fraud otherwise they would not be able to stay in business. The small amount of fraud occurring makes it difficult to undertake comprehensive analysis and therefore to formulate strategies based on that analysis.
- **It is well considered**: Successful fraud has often been well planned. It is very difficult for front office staffs dealing with customers to expect and detect them. These staff in most organizations are not well trained to detect it. Once fraudsters find a new modus-operandi they exploit it until discovered and blocked.
- **It is subtly concealed**: Fraud transactions show similar characteristics and patterns as genuine transactions. The Reporting Entities (REs) cannot easily differentiate between legitimate transaction and transaction involving fraud element.
- **It is time evolving**: Fraud keeps changing daily, weekly therefore it is challenging to devise strategies that can detect old, existing and new fraud. New modus operandi of fraud are seen evolving every day.
- **It is carefully organized**: A fraud incident typically leads to many fraudulent transactions. Social network analysis is needed to detect the fraud early in order to minimize the loss. Otherwise due to the involvement of many parties and quick transfer of the proceeds, the

[11] See more at Illicit Financial Flows from Cyber-enabled Fraud (2023) (fatf-gafi.org) https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

[12] Challenges in fraud prevention and money laundering detection: (Journal of Financial Compliance Vol1 No 1. Predictive analytics in fraud and AML. 2017

fraudsters may do huge loss in system before the fraud typologies, techniques are detected, and strategies are devised to tackle such fraud.

1.2.3 Money laundering techniques used in case of CEF

Cyber-enabled fraud has become significant international organized crime with dramatic increase in volume of recorded scams and global reach in recent years. These crimes can have a catastrophic impact on people, businesses, and economies around the world. Large financial losses from these frauds can erode public confidence in digital systems. Following techniques are seen employed by the fraudsters for laundering proceeds from fraud of this nature.

- The location in which the CEF occurs (i.e., where the victim is) is usually different from the location where the laundering of CEF-proceeds takes place. Similarly, money mule networks may be spread across nation and in larger syndicate it may be spread even in multiple jurisdictions. Similarly, accounts used to collect money from fraud are opened at one place of country and are seen operated from other place via online medium or via ATM or card-less withdrawal from different places. In few cases cash withdrawal is done via ATMs located at bordering markets of India as well.
- These fraudsters fear that Bank and Financial Institutions (BFIs) and Payment Service Providers (PSPs) may have already identified accounts used for fraudulent activity and debit freeze may have been imposed in these accounts. This could result in the interception of their criminal proceeds in these identified accounts before they can reach the destination accounts of fraudsters. To avoid criminal proceeds from being intercepted in frozen accounts, criminals carry out small value debit transactions to check if account is frozen so that they can change the destination of the funds if the account is frozen. Debit of amount as low as Re. 1 is seen in these accounts. Fraudsters are seen loading wallet accounts or topping up few common mobile numbers for this purpose.
- The choice of initial account utilized to receive proceeds from fraudulent activities often varies depending on the nature of the fraud. The aim is to portray the transactions as legitimate to the victims. But shifts have been noted over time in the type of initial account employed. For example, in case of BEC fraud, criminal groups have transitioned from individual accounts to corporate accounts to mitigate the risk of detection.
- After obtaining the unlawful cash, the fraudsters immediately funnel them into the money laundering network. The fund is then rapidly layered in the process using a series of account transactions involving both domestic and overseas accounts. Either the money mules or the fraudsters themselves control these accounts. Fraudsters gain control of an account when money mules hand over their banking credentials, cards, or grant power of attorney to the fraudster entity, allowing them direct authority over the accounts. This control is meticulously maintained so that transactions appear to be normal, concealing criminal behavior. These accounts are commonly used for a large number of sophisticated online transactions. Interestingly, many account holders seem to be uneducated or incapable of conducting such transactions themselves.
- To evade their detection and to remain anonymous, the fraudsters employ techniques like smurfing (i.e. breaking up large transactions into a set of smaller transactions that are each below the reporting threshold) and moving the funds across different financial institutions, remittance companies and PSPs. Conversion of proceeds of fraud to cryptocurrency or for online betting purpose too is observed frequently. The purpose is

to increase the time necessary for FIUs and LEAs to access and analyze the necessary financial data across sectors, and institutions making it difficult for tracing the funds, freezing the proceeds and recovering it.

- Sometimes money mule accounts are used for certain period of time only and thereafter no such transaction is done in these accounts. In such case it becomes difficult for financial institutions to identify unusual activity. In such cases, there is chance of fraud transactions to be masked by legitimate and regular transactions.

1.2.4 Vulnerabilities in social media for fraud

There are plenty of social media sites from like Tiktok, Instagram, Facebook, Twitter, LinkedIn, and many more to select from today — and the same is true for scammers wanting to launch their next assault. Same person uses social media accounts in multiple devices. Information shared by people on social media and their interaction in social media platforms are facilitating scammers. Some of the dimensions of some social media platforms that are facilitating scammers are as below:

- Social networking networks allow for several profiles and accounts without identification verification, allowing fraudsters to create false identities to defraud potential victims.
- Social media users often reveal details of their personal lives to public. Scammers can use this information to manipulate their victims. Such information includes age, date of birth, occupation, identity numbers like citizenship and driving license number, friend circle, recent places visited, social media pages liked and followed etc.
- Social media has become a common way for companies and brands to communicate with potential customers. Scammers are taking advantage of that to make contact with potential victims. These frauds are so meticulously executed that even well educated people become prey to the frauds.
- Scammers take advantage of the sense of desire and envy that social media platforms foster, by frequently exhibiting photos or videos of affluent lifestyles to lure their victims into a shot at this life if they participate in their fraud. In recent time, many Nepalese people are falling prey to such appeal, especially in online job frauds, where they are made to operate their bank accounts in favor of fraudsters or they hand over the control of their bank account to fraudsters.

1.2.5 Vulnerabilities in payment systems for fraud:

Social distancing practiced during COVID-19 Pandemics has increased the popularity and use of digital medium for payment all around the world. Digital medium for retail payment has increased rapidly after COVID-19 in Nepal as seen from table below.

Table 1-1 Access on Payment Systems

S.N.	Particulars	Mid-August 2020	Mid-May, 2024	% Change
1	Wallet Users	6,274,129	22,615,122	260.45
2	Debit Cards	7,437,602	12,789,656	71.96
3	Credit Cards	164,386	286,253	74.13
4	Mobile Banking Customers	11,464,867	23,797,680	107.57
5	Internet Banking Customers	1,045,558	1,938,888	85.44
6	connectIPS Users	162,117	1,251,440	671.94

Source: Payment Systems Department, NRB

Significant rise in users of connectIPS, wallet, mobile banking, internet banking and cards is seen during the period of around four years.

Increased adoption of information technology in payment systems has created more opportunities for fraud. A study of Boston Consulting Group on payments security found following vulnerabilities in U.S. Payment System [13] that is very insightful for Nepalese payment industry as well:

- Increased use of relatively new channels, use of multiple devices and increased system connectivity offer more endpoints for fraudsters to exploit the payment systems via use of sophisticated technology.
- The participants of payments system have varied resources and capabilities to combat fraud. Fraudsters target the weakest links and highest-return opportunities in the payments ecosystem, such as susceptible endpoints, people, technology, and organizations with insufficient fraud-fighting resources and/or experience.
- Fraudsters are constantly developing alternative types of attacks and searching for new vulnerabilities within the payment system. Collaboration among the stakeholders is necessary to identify fraud patterns, take steps to limit those types of transactions. But comprehensive fraud data are not shared timely across the payment industry. This limits the ability of stakeholders to even compare their loss experience with that of others.
- Individual stakeholder incentives may be misaligned or insufficient to reduce collective fraud losses. Coordinated action by all payments stakeholders is required for successfully reducing fraud. So balance in competing priorities must be in line to reduce fraud in system.
- Organizations rely on static data like national identity number, address, account numbers, card expiration dates for enrolling customers, verifying identity, access accounts and authenticate transactions. These static data that are often compromised. With the increasing prevalence of data breaches and their oversharing on social media much of this information is readily available to for fraudsters.
- Human error is an important element in CEF in payment systems. People play a critical role in maintaining the security of the payments process. Yet consumers and employees can fall prey to fraudsters if they don't understand the risks and how to prevent fraud.

Many studies agree that human error/greed contribute huge portion of all cyber security breaches. According to the World Economic Forum ninety-nine percent of all cybersecurity issues can be traced to human error[14]. According to an IBM assessment, human error is involved in 95% of information security errors.[15]

The ease of mobile SIM clone fraud has also created vulnerability in payment systems. The mobile number is used for one-time password (OTP) and two factor authentication. It is also used as credential for getting access to account of customers. If mobile service providers are tricked into

[13] Executive Summary A View of Payments Security: Trends, Gaps and Vulnerabilities; Boston Consulting Group's review of academic literature, surveys and industry reports on fraud and associated costs. (http://fedpaymentsimprovement.org/)

[14] See more at https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/

[15] See more at IBM Security Services 2014 Cyber Security Intelligence Index (https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF)

providing existing mobile SIM number to the fraudsters they can easily access the account of customers.

Unrealistic target from management of BFIs for enrollment more and more customers to wallets, mobile banking, internet banking and other digital payment products have also resulted in more people being vulnerable to various schemes of frauds. Fraud cases do not always arise from the error from the customer side. International experience shows that it may also arise due to misconduct of the bank staffs as seen in Bank of Baroda App scams (as shown in box below).

Box 1. Bank of Baroda App Scam.

In July 2023, a media report revealed that the process of signing up customers for Internet banking app of Bank of Baroda was fraudulent. The employees at certain Bank of Baroda branches allegedly linked customers' bank accounts with unrelated mobile numbers and enrolled them on the "Bob World" app.

This mobile app, similar to other banking apps, offered customers various digital banking services, including loan access, savings, investment options, bill payments, and even booking buses and hotels. According to the report, with a huge target from management for enrolling existing customers to the app, bank employees resorted to linking bank accounts without associated mobile numbers to the contact details of various personnel, including staff, sanitation workers, and security personnel to meet demanding sign-up targets for the digital app. After the initial registration, these employees would then deregister the bank accounts from the app and reuse the same mobile numbers to link a different set of bank accounts.

While Bank of Baroda initially denied these allegations, it later initiated an internal audit in response to the accusations. RBI later banned the bank from onboarding new customers to the app. The RBI mandated that the Bank of Baroda, the seventh largest in India by market cap, sign in new customers to the BoB World app only after it rectifies the identified issues and strengthens the relevant processes to the regulator's satisfaction. In response to this, the Bank of Baroda has taken action by suspending certain employees and launching an investigation to establish accountability.

Linking unauthorized mobile numbers exposed customers to the risk of fraud as the person with the registered mobile number gains access to the account. Bank of Baroda's internal audit has later uncovered a theft of Rs 22 lakh from 362 customers, with six individuals losing more than Rs 1.10 lakh.

Agents, known as business correspondents, linked mobile numbers on the customer's consent forms to on-board them on to the 'Bob World' app apparently due to pressure from the bank to boost registration on the Bob World app. But then these agents stole money from the customer accounts through un-authorized mobile linking.

Source: Aljazeera.com https://www.aljazeera.com/economy/2023/7/11/indias-bank-of-baroda-misused-customer-data-to-flog-app

1.3 Scope of the study

As discussed in introduction section, the term fraud is broad and can be classified in numerous ways. For the purposes of study CEF is defined as one which originated online (e.g. watched advertisement online, got a message on social media) even if it involved offline activity later.

This report focuses only on illicit financing arising from such fraud that is enabled through or conducted in the cyber environment that involves

(i) National and transnational flow of funds
(ii) Deceptive social engineering techniques (i.e. manipulating victims to obtain access to confidential of personal information).

There are many variations of frauds involving these elements. This report focuses on frauds like BEC fraud, social media and telecommunication impersonation fraud, online trading/ trading platform fraud, online romance fraud, employment frauds etc. collectively referred as CEF. The report has included the study of frauds of above nature i.e. enabled through or conducted in the cyber environment as far as possible. However, illicit financing related to ransomware and other malware-enabled crimes are not within the scope of this report.

The report is prepared based on reported STR/SAR at FIU-Nepal, trends and typologies of CEF observed in STR/SARs, data provided by Nepal Police and Office of Attorney General. The study also tries to provide recommendation for future action to REs, regulators, LEAs and other stakeholders in order to minimize risk of CEF.

1.4 Objectives of the study

The primary objective of the study is to understand money laundering and terrorist financing risk associated with CEF. Specific objectives of the analysis are:

- To enhance understanding of the threat posed by CEF.
- To identify significant and emerging trends of CEF based on STR/SARs reported at FIU-Nepal involving various customer, products, delivery channels and geographies involved.
- To develop the red flag indicators which will assist the REs to identify CEF.
- To provide recommendation to REs, regulators, LEAs and other stakeholders to counter CEF.

1.5 Methodology of the study

The methodologies adopted for the study are listed in points below:

- REs select one or more indicators among thirty-two predicate offence indicators while submitting STRs/SARs in goAML software. Only those STRs/SARs, which are linked to indicator "fraud", are considered for the purpose of analysis in this study.
- The study is done in a descriptive format where findings from the available STR/SARs are shown in percentage, average and summation model. General overview of fraud related STR/SARs is presented from the study of STR/SARs received, analyzed and disseminated using goAML software between Jan 1, 2020 to May 31, 2024.
  For detailed analysis of recent CEF related STR/SARs, all the CEF related STR/SARs reported in first five months of year 2024 were identified. From among 319 such identified STR/SARs,

a sample of 151 STR/SARs was taken using random sampling method and analyzed by going through description and observation of REs along with provided attachments.

- Besides the data that are reported by the REs, data from the FIU-Nepal's own operational intelligence and tactical information, information from Nepal Police, Office of Attorney General, other government agencies and public sources and is used for analysis.
- Different publications of FATF, APG, FIUs of different jurisdictions, INTERPOL, Nepal Police, Office of Attorney General and organizations involved in cyber security were referred during the analysis.

1.6 Limitations of the study

Limitations encountered in the study are listed in points below:

- Study is based on STR/SARs in which at least one of the selected predicate offence indicators was 'fraud'. The classification of reports under predicate offence 'fraud' is solely based on the judgement of the REs.
- Fraud is broad term and can be closely related to other predicate offences as well. As multiple indicators can be selected for any STR/SAR, the indicator fraud may have been selected for suspicious transactions related to other predicate offences as well. Conversely, instead of selecting the indicator 'fraud', offence indicators like, 'Money, banking, finance, foreign exchange, negotiable instruments, insurance, cooperative related' or 'Forgery' might have been selected by REs.
- Due to limitation of time and resources, detail contents of fraud related STR/SARs received in first five months of year 2024 only were reviewed to isolate STR/SARs related to CEF from other fraud typologies. Among the CEF related STR/SARs received, sample of only 151 STR/SARs was studied in detail to draw conclusion.
- Availability of published data of cases categorized under CEF was limited at LEAs. Similarly, data of prosecution/court judgement related to frauds classified under CEF was also limited.

2. Legal provision on fraud/CEF, modus operandi of CEF, cases of fraud/CEF in Nepal and their reporting at FIU Nepal

2.1 Legal provision to curtail fraud/CEF in Nepal

In Nepal National Penal (Code) Act 2017, section 249 has prohibited committing cheating. As per the code, 'a person who dishonestly causes any kind of loss, damage or injury to another person whom he or she makes believe in some matter or to any other person or obtains any benefit for him or her or anyone else by omitting to do as per such belief or by inducement, fraudulent, dishonest or otherwise deceptive act or preventing such other person from doing any act shall be considered to commit cheating'. A person committing the offence is subject to sentence of imprisonment from seven to ten years and fine up to one hundred thousand rupees depending upon victim and method of cheating. Additional sentence of up to one year shall be imposed in the case of cheating a child, person of unsound mind, helpless, illiterate or person above seventy-five years of age. Regarding the compensation to victim of this crime, the claimed amount, if set out, and a reasonable compensation, if the claimed amount is not set out, shall be ordered to be paid by the offender to the victim. However, no complaint shall lie after the expiry of one year from the date of knowledge of commission of this offence.

Fraud is one of the 32 predicate offence as per clause 2(ad) (Annexure-1) of the Asset (Money) Laundering Prevention Act (ALPA), 2008. Fraud has been classified as Medium Risk area in National Risk Assessment Report on Money Laundering and Terrorist Financing, 2020. Banking Offence and Punishment Act 2008 is specialized law in place for banking sectors fraud.

Electronic Transactions Act 2008 has provision for punishment if computer fraud is committed. As per the act amount of financial benefit acquired from computer fraud shall be recovered from the offender and be given to the person concerned. Offender shall be liable to the punishment with a fine not exceeding one hundred thousand rupees or with and imprisonment not exceeding two years or both.

Central Investigation Bureau (CIB) and all police offices which have authority to take first incident report (FIR) handle the crimes involving fraud. There are total of 292 offices where lawsuit for fraud are initiated. Complaints for CEF can be reported and registered at Cyber Bureau, District Police Ranges and all remaining 74 District Police Offices.

2.2 Modus operandi of commonly used CEFs typologies with examples/cases

Fraudsters employ various CEF typologies to deceive people. Some of the common fraud typologies observed in Nepal are presented below along with related cases. Sources for the cases are mentioned where applicable. Identity of persons and institutions are hidden in those cases which are based on STR/SARs received by FIU-Nepal.

- **Business Email Compromise (BEC) fraud:** Victims receive email instructions that is meant to be from their clients or suppliers' asking victims to transfer funds to new payments accounts. BEC is a specific type of spear phishing attack where the scammer uses email to trick someone into sending money or divulging confidential company information.
  To carryout BEC scammer might spoof an email account or website, send spear phishing emails and use malwares that can infiltrate company networks and gain access to legitimate

email threads about billing and invoices. In case of international trade, money is sent to different jurisdictions creating difficulty to track and freeze the fund.

Box 2. BEC fraud on Nepalese importer firm

ABC Pvt. Ltd. is an importer and distributor of computer and computer related accessories located in Kathmandu. The company regularly imported items from an exporter XYZ Pvt. Ltd. based in Singapore and made payment from a bank in Nepal. On November 2019, ABC Pvt. Ltd. received a Performa Invoice in e-mail, seemingly from XYZ Pvt. Ltd. Bank account detail of exporter was changed in the Performa Invoice from CITI Bank, Singapore to LLOYDS Bank PLC, United Kingdom. On request of the client, the bank in Nepal transferred the invoice amount $ 17,520.00 to LLOYDS Bank PLC, United Kingdom, for the import hard disks from Singapore . But XYZ Pvt. Ltd. did not receive the payment.

Upon inquiry, it was found that the email regarding Performa Invoice was fraud and email of Sky Nepal was hacked. The email regarding Performa Invoice was spear phishing email and hackers changed bank account details from CITI Bank, Singapore to LLOYDS Bank PLC, United Kingdom. The account at LLOYDS Bank PLC, in which fund was transferred, was found to be of an Individual. When ABC Pvt. Ltd. communicated with Lloyd's Bank regarding the fraud amount, the bank suggested the customer to go to the remitting bank and send swift to 'call bank funds under scam'. Until then most of the transferred amount was already withdrawn. Hackers had also sent spoofed emails to XYZ Pvt. Ltd. appearing like they were sent from ABC Pvt. Ltd. Such email domains were blocked after discovery of the incident.

- **Phishing fraud:** Victims are deceived into revealing sensitive information such as personal data, banking details or account login credentials. The criminal will then use the information to drain the victims' money from their account, open new accounts or make fraudulent transactions. Fraudsters create a third-party phishing website that appears to be a genuine website, such as a bank's website, an e-commerce website, or a search engine.
  Fraudsters call or approach customers via phone or social media, posing as bankers, company executives, insurance agents, government officials, and so on. Imposters share a few customer details, such as the customer's name or date of birth, to gain trust.
  In some cases, imposters pressurize/ trick customers into sharing confidential details such as passwords / OTP / PIN codes of cards/ Card Verification Value (CVV), etc., by citing an urgency /emergency such as the need to block an unauthorized transaction, payment required to avoid some penalty, an appealing discount, etc. The fraudsters then deceive customers using these credentials.

Box 3. Prithvi Bahadur Shah arrest: Here's how he allegedly deceived an American

Stephen Farmer, who lives in northern California of the US, has accused Shah of illegally bringing USD 350,000 that he withdrew to Nepal. Stephen Farmer's father, James Farmer, was supposed to get USD 481 from a defunct company. A man named James Morgan contacted him claiming that he can return the money. Stephen's account received a notification of a deposit of USD 481,000 instead of just USD 481. He hence contacted James Morgan after receiving the notification, but it turned out that the notification was fake.

But, Mr. Morgan claimed that the transaction was a mistake; Mr. Stephen took out USD 350,000 of it, as per the agent's instructions, and deposited it into the Times Today Peace Holiday Environment Pvt account at Durbarmarg-based Kumari Bank.

After the amount was paid, the bank contacted Stephen Farmer. After that conversation, he figured that the previous deposit was fake. He requested the bank to cancel the transaction, but, by then, it was too late.

He was in regular contact with the bank, and the bank claimed he could get the money back. The American bank also tried to intercept the transaction while reaching out to Kumari Bank Ltd. But, the transaction was already done and got a stay order from the Nepal Rastra Bank.

Source: Onlinekhabar.com (https://english.onlinekhabar.com/prithvi-bahadur-shah-nepal-fraud-case.html)

- **Social media and telecommunication impersonation fraud:** This includes scenarios where fraudsters contact victims via mobile or social media applications by criminals pretending to be government officials, relatives or friends. Fraudsters then prey on the victims' emotions to induce payment or hand over control of payments accounts or to carry out financial activities such as a loan application or an account opening to receive criminal proceeds. Fraudsters create bogus accounts on social media platforms such as Facebook, Instagram, and Twitter, among others.
  Fraudsters will then send a request to the users' friends for money for urgent medical needs, payments, and so on. Fraudsters contact users and gain their trust over time by using forged information. When users share their personal or private information, fraudsters use it to blackmail or extort money from them.

Box 4. Government of Nepal Vs Arjun Saud

[Case no.: 074-C2-0161; Victim: Bhojraj Thapa; Defendent: Arjun Saud]

Bhojraj Thapa, a journalist, filed a complaint stating that an unknown person had created a fake Facebook profile in his name. This fake account posted a plea for donations, claiming Thapa's child was seriously ill and needed funds for treatment. Thapa requested legal action against the individual responsible for this fraud.

Arjun Saud confessed to creating the fake Facebook account and using Thapa's name and photos to solicit money from others. Saud admitted to using the social media platform to deceive people into sending him money via mobile payment services such as e-Sewa and NIC Asia Bank. The total amount fraudulently obtained was NPR 283,026.11.

The court found Arjun Saud guilty of violating the Electronic Transactions Act, 2063, and the Criminal Code Act, 2074. Saud was sentenced to 6 months in prison, a fine of NPR 56,000 and additional penalties of NPR 2,200 for victim compensation under the Victim Protection Act, 2075. The decision allows for an appeal to be filed within 70 days in the High Court Patan.

- **Online business / trading platform fraud:** Victims are deceived by fake advertisements or advisors online to non-existent or fake platforms for trading or investment related to both fiat and virtual assets. Fraudsters pose as seller of goods at an attractive price in social media sites like Instagram and Facebook. When buyer approach these web pages and order for goods, sellers trick buyers into making pre-payment on different pretext e.g. they have to first order

goods from other party and they are short of cash. When the amount is deposited in seller's account, they block the buyers and goods is never delivered.

People are also tricked into investment in virtual assets like cryptocurrency. The advertisements direct the potential prey to deposit amount in certain bank accounts or wallet accounts. The amount thus deposited is later not returned as promised. In countries like Nepal where investment in virtual assets like cryptocurrency is illegal, the victims rarely come up with complaints against such scams for potential repercussions.

Scammers may sometimes also pose as buyers on online sales platforms expressing an interest in the seller's product. e.g. in India scammers trick sellers into using the Unified Payments Interface Unified Payments Interface (UPI)'s app's "request money" option instead of paying the seller using "send money" option. When the seller approves the request by entering the UPI PIN money is transferred to the fraudster's account.

Box 5. Scammed by person posing as collector of ancient coins in social media

A walk-in customer named Ms. STM visited Satdobato Branch of Bank X and informed that she was victim of online scam. On 12th April 2022, she had transferred total NPR. 70,000.00 into the account of Ms. NC maintained at Bank X from her mother Mrs. MTM's account maintained with Bank Y.

As per Ms. STM she met a person named Mr. BW over social media who identified himself as an avid collector of Nepalese and Indian ancient coins and bank notes. After communicating with the person online, the collector ordered coins and notes and Ms. MTM sent coins and notes to given address. Later, the collector Mr. BW requested Ms. STM to deposit courier and insurance charge into the account of Ms. NC, which he said, will be refunded later along with payment proceeds of ancient notes and coin. Ms. STM deposited Rs. 70,000 as mentioned above on account of sale of ancient coins and notes. However, no payment was made from other side as promised.

After the Bank X received the complaint, an enquiry was made by bank about Ms. NC whose account was credited by Ms. STM. It was found that Ms. NC was also a victim of social media fraud. She had opened bank account and provided mobile banking credentials to same person Mr. BW. Ms. NC informed that she was unaware of transactions being performed in her account which were mostly conducted through the digital platform.

Later Ms. STM recovered fully the transferred amount Rs. 70,000.00 from Mrs. NC with the help of Nepal Police. Out of total amount Rs. 411,143.10 credited in account of Ms. NC, Rs. 254,500.00 was found transferred to another bank 'Bank Z' via Fonepay on four different dates and NPR 10,000.00 was found transferred to Ms. NC own wallet account. This shows that there might be some other victims also who have deposited amount in the accounts of Ms. NC.

- **Online romance fraud:** Romance scammers tell all sorts of lies to steal heart and money from target. These scammers pay close attention to the information target share, and try their best to become perfect match for victim. Contact starts with target on social media, website or dating app and then they quickly move to Whatsapp, Messenger, Viber etc. Victims are tricked into sending money to criminals after being convinced that they are in a romantic relationship. The scammers find reasons for unable to meet physically and these reasons are well concealed by their fake identity. For example, they may claim themselves as working faraway in military

base or in a project abroad with less chance of leave. It is one of the lowest reported types of online fraud because victims can be ashamed to come forward, or may be unaware or unwilling to accept that they are victim. Fake profiles on social media or online dating sites are set up with stolen photos, fictitious names and occupation to contact possible victims. After establishing the trust the perpetrators request for financial assistance. They may give reasons for need of such funding like medical emergencies, being unable to access their own money in foreign countries due to frozen bank account, taxes/customs imposed by other countries, money needed for inheritance fees etc. More vulnerable persons of such frauds are usually senior citizens, widowed, separated or divorced persons.

- **Employment fraud:** Fake job offers on social media platforms trick victims to pay scammers upon various excuses including advanced payment for purchasing commodities to boost sales of a trading platform or a guarantee fee to secure employment. When job seekers share secure credentials from their bank account, credit card, or debit card on these websites during registration, their accounts are compromised.
  Fraudsters may also pose as representatives of reputable companies and offer employment after conducting bogus interviews. The job seeker is then persuaded to transfer funds for registration, mandatory training, a laptop, and other expenses.

Box 6. Employment scam used for operating money mule account

Mr. DG registered a complaint at Bank X via email mentioning that he was victim of online fraud. Fraudster was an individual who identified himself as Mr. EE from Detriot, Michigan. As per the email the foreigner and two Nepalese, namely Mr. SK and Mr. BK were involved in online fraud. The accounts of Nepalese were used to collect money from fraud.

Mr. SK is one of customers of Bank X who opened account in Arughat branch of the bank only few days before the complaint was received. High volume of electronic transactions was observed while reviewing his account.

When the branch carried out an enquiry with Mr. SK about the transactions in his account, he informed that he met a person named Mr. GW on Instagram and had conversation with him. Mr. GW then offered him a marketing job. He asked for bank account number and mobile number of Mr. SK saying that it was requirement to deposit salary in account. However, the fraudster shared the account number of Mr. SK to victims of online fraud to deposit amount in different pretexts. The fraudster Mr. GW then used the account credentials and conducted debit transactions from Mr. SK's account by asking for the OTP sent in account holder's mobile number. Mr. SK gave OTP every time fund was transferred from his account unknown to the fact that fraudulent transactions were being carried out in his account. In this way both Mr. DG and money mule account holder Mr. SK were victim of online fraud.

- **Lottery fraud:** Most scams work by offering the victim an easy way to earn a chunk of money, or the chance to win a valuable prize or get something for free or at a huge discount. The main goal of this type of threat is to raise money, but scammers can also harvest the victim's personal data to sell later or use in other schemes. Scammers send emails or make phone calls claiming that a customer has won a large lottery prize. In order to receive the lottery amount customers must confirm their identity by entering their bank account, credit card information,

e-mail address, date of birth, gender, phone number, home address etc. on a website from which the fraudsters collect data.

Customers are also required to pay taxes/forex charges/upfront or to pay shipping charges, processing / handling fees, and so on. In some cases, fraudsters will pose as an representative of bank, customs, or a representative of a foreign bank/company/international financial institution and ask the customer to transfer a small amount in order to receive a larger amount in foreign currency from that institution.

Box 7. Lure of easy money leads Nepalese into traps of online fraudsters

A 40-year-old man from Pokhara with 'Rana' surname, who owns a small business in Pokhara, got a message on WhatsApp. The message said one 'Alex Clork Rana' had died in Canada a few years ago, and there was no one to claim his $78 million lying in the Royal Bank of Canada. The message urged the receiver to withdraw the huge sum, while congratulating him on his good fortune to be bestowed a fortune. Mr. Rana was taken into confidence by the fraudster, who further told him that he could easily give evidence to the bank of the Pokhara man's link to Alex Clork Rana. The bank would then hand over the money to him as soon as the verification formalities were completed.

Initially, Rana was asked to send $1,500 in order to hire a lawyer for the purpose. Then, on various other pretexts, he was made to send large sums to 11 different individual bank accounts. When he lodged a complaint to Cyber Bureau, Bhotahity, he had already sent $78,000 (equivalent to around Rs 10.2 million) to the fraudster from different bank accounts, all from Pokhara.

Source: The Kathmandu Post, Published : April 25, 2023 (https://kathmandupost.com/national/2023/04/25/lure-of-easy-money-leads-nepalis-into-traps-of-online-fraudsters)

- **Parcel/ Courier fraud:** Parcel scams typically involve unsolicited contact about a supposed parcel delivery. Scammers pose as a legitimate courier company, customs official, or even a Law Enforcement Agency (LEA) to trick people into believing they are receiving a parcel.

  An email or text message is received from sender that claims to be from a reputable delivery service with convincing communication. The message may state that the recipient is expecting a parcel or that there are problems with the parcel during transit. The victim is then asked to provide sensitive personal information or financial information, or to pay for customs fees or parcel charges. The scammer may also direct victims to fake websites that are concealed as a legitimate courier service. The scammer may also use a fake phone number or official logo to increase the credibility of the scam. They take advantage of people's trust in delivery systems and exploit their desire to resolve apparent delivery issues quickly. Variations of parcel scams include unclaimed package scam, fake customs scams, phishing scam, OTP scam, WhatsApp scam.

Box 8. Person claiming to be from Syria sends message to random person and tells she has sent box full of cash in his address using diplomatic courier

On July, 2024 Mr. JN received message in Facebook messenger from Ms. EA which mentioned that she is sending huge amount of cash from Syria to Nepal as a diplomatic parcel. She then told Mr. JN that she is willing to give thirty percentages of that amount if he helped collect the fund. She also told that she was in mission with Syrian government and she will visit Nepal within

three months. She urged Mr. JN to provide his name, address, and phone number immediately as parcel was being sent very soon.

After he provided name and other details Ms. EA sent him photo of airway bill showing parcel being sent in his name and address. She requested him to keep everything secret between two of them. After few days Mr. JN received message from unknown person in Whatsapp. The person in message, who claimed to be diplomat of Ms. EA, told him to deposit customs charge in order to release the parcel from airport. Ms. EA too inquired about the message that the diplomat sent him in Whatsapp. Later they shared account of Mr. IR telling that it is the account provided by the customs in order to release the parcel.

Mr. JN visited Manamaiju Branch of the bank inquiring about courier dispatched and payment option to be made to our customer named Mr. IR. Observing the transaction history in the account, branch staffs suspected that the customer Mr. IR may be involved in fraudulent activity. Bank lodged STR to FIU-Nepal mentioning the incident along with bank statements and screenshots showing conversation in Facebook messenger between a foreigner named Ms. EA and Mr. JN related to courier delivery.

Bank statement of Mr. IR shows transactions done mainly using digital medium such connectIPS, Fonepay IBFT, Khalti wallet and others. Credited fund is immediately transferred through digital modes to his own account maintained at another Bank leaving the account balance very low. Credit and debit transactions in account is around Rs. 19.82 lakhs each within three months of account opening. Frequent single digit debit and credit transactions is seen in the account which is suspected of being carried out in order to test whether accounts are debit restricted by Bank or not. Such single digit credit and debit transactions are carried out between same 3-4 persons frequently. Similar transaction pattern is seen in the bank accounts of these other persons with whom Mr. IR has regular transactions and these accounts too are suspected of being used to park the fund earned from fraudulent activities.

- **Free iPhone fraud:** The "You've won an iPhone" phishing scam relies on the excitement around Apple's latest iPhone models to trick unsuspecting users into providing personal information and payment for shipping charges and custom duty. Scammers send text messages, voice messages or emails pretending to be from well-known retailers like in Dubai or other cities. These messages congratulate the recipient on winning an iPhone in a special giveaway or contest. The video clips in Tiktok and other social medias showing free giveaways of iPhone by different stores has further helped enhance the success of fraudsters in tricking users of social media into this scam.

Box 9. Law firm employee loses ₹2.9 lakh to free iPhone fraud

The victim, Supriya Ghadi, who works for a compliance and labour law consulting firm in Lalbaug, India was targeted by fraudsters, who called her after she had liked videos of Zam Zam Electronics Trending of Dubai on Instagram. According to the complaint registered at police station Ms. Supriya was contacted by some unknown people via phone posing as employees of Zam Zam electronics. What followed was a series of fraudulent offers and demands, which eventually ended up costing Ms. Supriya a sum of ₹2.9 lakh. The fraudsters told her that she had won a free iPhone 14 Pro handset but said she will have to buy a ₹3,000 coupon to get it. The accused even sent a photo of the coupon to her. Ms. Supriya paid him the money via Gpay.

The accused contacted her again and told her that she had also won an Apple Watch and headphones for which she will have to pay courier charges of ₹25,000. She transferred the amount accordingly. They called her yet again and told her to transfer more money for iPhone registration and its fast delivery. Later, they told her that she had won one more set of the three Apple products — iPhone 14 Pro handset, Apple Watch and headphones, and she will have to pay ₹60,000 for the same. The fraudster kept her asking for money in the pretext of currency conversion, iPhone ID, custom duty, parcel charge and so on and she kept paying for it. When she realized that she was victim of fraud she decided to approach the police for help.

Source: Hindustan Times https://www.hindustantimes.com/cities/mumbai-news/mumbai-woman-cheated-of-2-9-lakh-after-liking-dubai-based-electronics-shop-s-instagram-page-101684870296764.html

- **Use of unknown/unverified mobile apps:** Fraudsters distribute app links disguised to look like the existing apps of authorized entities via SMS, email, social media, and instant messenger, among other channels. Customers are duped into clicking on such links, resulting in the installation of unknown/ unverified apps on their mobile /laptop/ desktop, and so on. The fraudster gains complete control of the customer's device once the malicious application is downloaded. These include confidential information stored on the device as well as messages/OTPs received prior to and after the installation of such apps.

- **Fraud using screen sharing app and remote access:** Victims are tricked into downloading a screen sharing app. Using such an app, fraudsters can monitor/control the customer's mobile/laptop and gain access to the customer's financial credentials. Fraudsters use this information to conduct unauthorized funds transfers or payments using the customer's internet banking/payment apps. Screen-sharing frauds involve cyber-criminals tricking individuals into sharing access to their computer screens or devices. These scams often occur during tech support or remote assistance scenarios, and scammers exploit the victim's trust to gain unauthorized access.

Box 10. Half of investors would miss signs of screen sharing scam as Financial Conduct Authority (FCA) warns

A 59-year-old who was persuaded to download remote desktop software to secure an investment, lost over £48,000 while scammers accessed her banking details, her pension, and applied for loans on her behalf. Angela Underhill clicked on an advertisement for bitcoin and received a call from individuals claiming to be financial advisers. Offering to complete the first investment for her, they asked her to download the 'AnyDesk' platform, which then gave the scammers open access to all the financial details on her computer.

Her case is just one of thousands the Financial Conduct Authority has seen reported to its Consumer Helpline with over £25 million lost between 1 January 2021 and 31 March 2022 and victims age ranging from 18 to over 70. Using platforms including Teams, TeamViewer and Zoom, screen sharing scams not only involve consumers sharing their financial data – but scammers have also been able to embed themselves in victims' digital devices to access online banking and investment details.

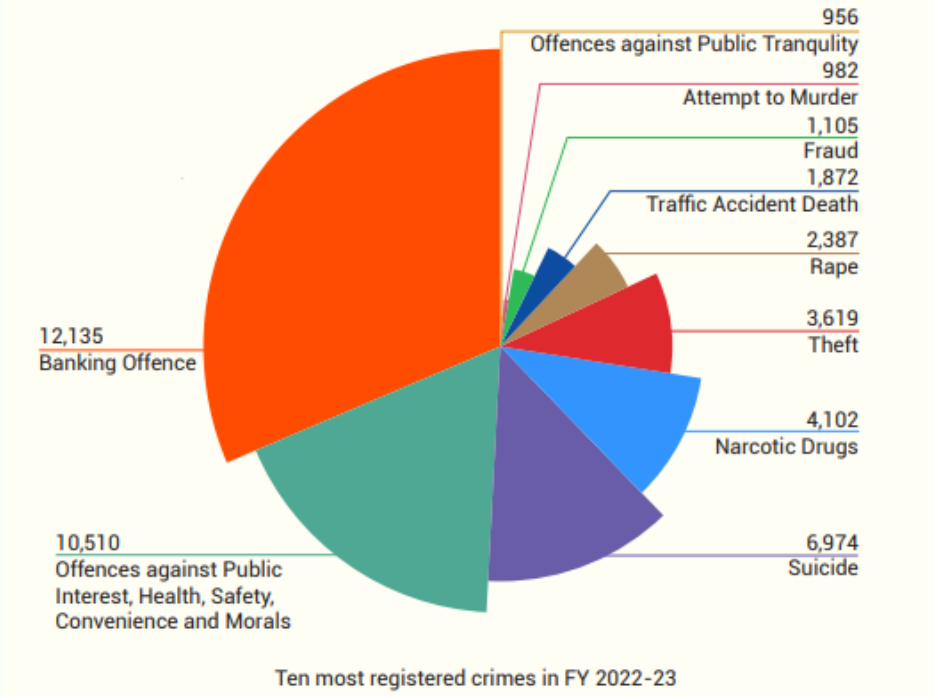
Source: Financial Conuct Authority, https://www.fca.org.uk/news/press-releases/investors-miss-screen-sharing-scam-signs

- **Charity scams:** These frauds leverage on emergency situations and collect money from people making them believe that they are donating to charities. Charity scammers may ask for donations on the phone, SMS, by e-mail, or through social media. Rise in such scam was visible during the COVID-19 pandemic, the Russia and Ukraine conflict, and the earthquake in Türkiye and Syria.

2.3 Fraud/CEF cases in Nepal

As per crime statistics of Nepal Police, fraud is one of the ten most registered crimes in Fiscal Year 2022-23. Banking offence was highest registered crime during the period.

Figure 2-1 Ten most registered crimes in fiscal year 2022-23 at Nepal Police

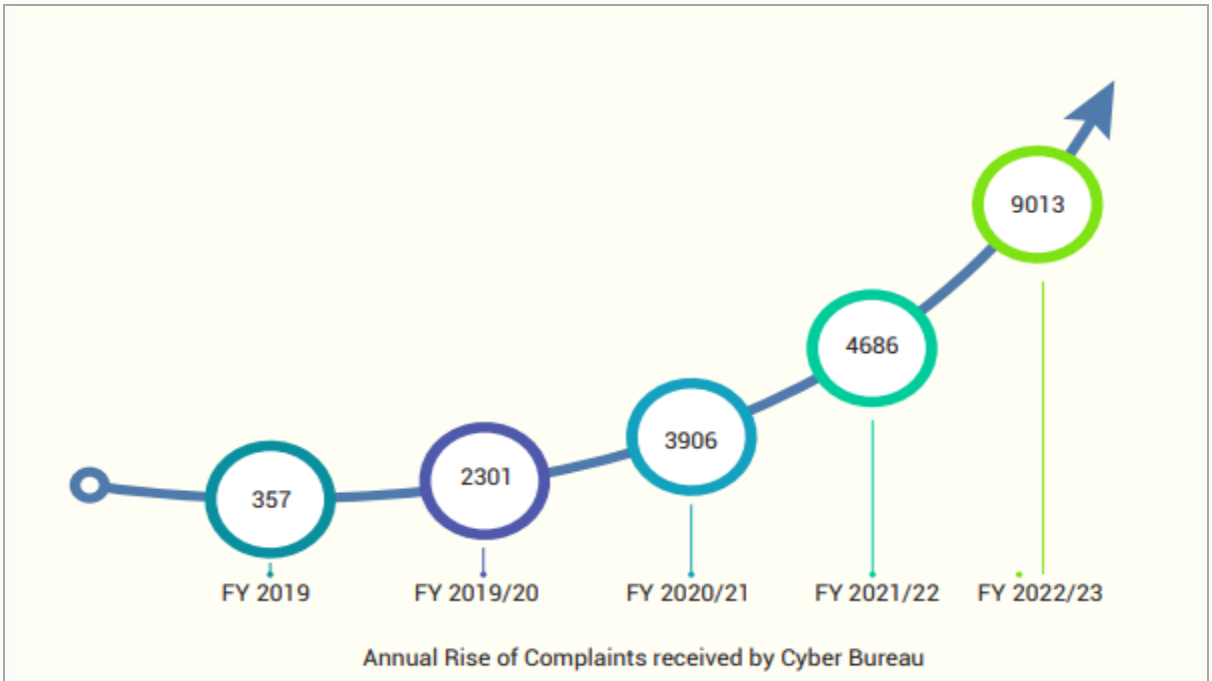


Source: Police Mirror (2023)

Cyber Bureau is a specialized unit of Nepal Police, dedicated to analyze Cyber Security and curb Cybercrime in Nepal. The Bureau acts as a focal unit on cyber issues. As per the Police Mirror 2023, there is steady rise in complaints received by Cyber Bureau over the years.

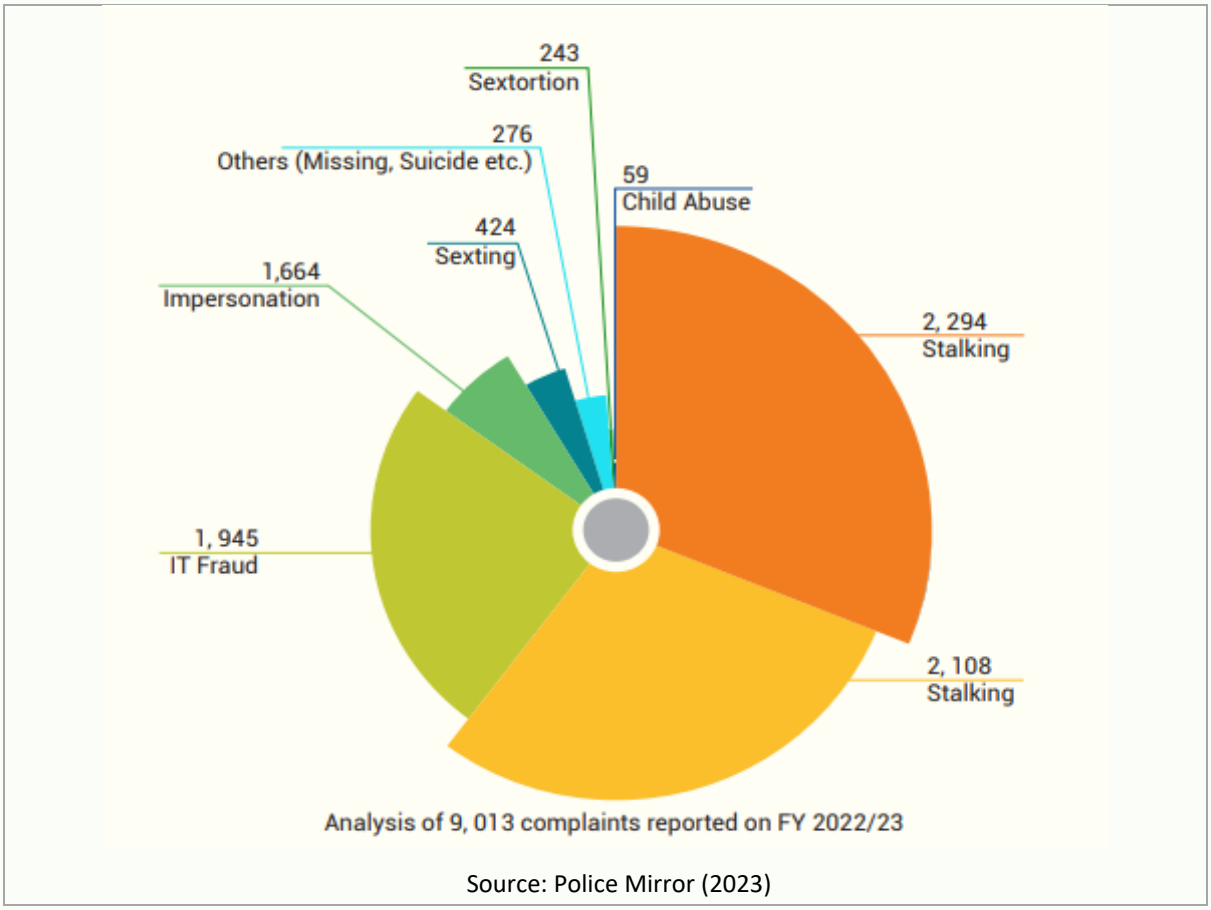
Of the 9,013 complains received by Cyber Bureu, 1945 complains were about IT related fraud as seen in figure below. The financial crimes include phishing (attempting to acquire sensitive data such as bank account numbers in a guise), lottery scam including alluring fraudulent offers of work from home and online shopping.

Figure 2-2 Trend of complaints received by Cyber Bureau of Nepal Police



Source: Police Mirror (2023)

Figure 2-3 Analysis of complaints received by Cyber Bureau in Fiscal Year 2022/23



Source: Police Mirror (2023)

As mentioned in Mutual Evaluation Report of Nepal (2023), Nepal Police has frozen sum above 110.1 million rupees and seized sum above 21.3 million rupees related to fraud during the period of 2017-2022 (Figure 1-4).

Figure 2-4 Nepal Police's freezing/seizing actions in predicate crime cases

	Predicate Crime	Estimated value of freezing in NPR	Estimated value of seizing in NPR
2017-2022	Human Trafficking	50,000.00 (~USD375.00)	50,000.00 (~USD375.00)
	Narcotics	3,208,537.95 (~USD24,000.00)	3,597,496,668.98 (~USD27,000.00)
	Fraud	110,141,454.34 (~USD826,000.00)	21,346,833.05 (~USD 160,000.00)
	Bank Offences	Nil	98,874,055 (~USD 741,000.00)
	All other predicate crimes	82,837,954.00 (~USD 621,000.00)	178,880,515.62 (~USD1,341,603.00)
	Total	**196,237,946.29 (~USD 1,471,784.00)**	**3,896,648,072.65 (~USD29,614,525)**

Source: Mutual Evaluation Report of Nepal (2023)

As per Central Investigation Bureau (CIB), total 4,112 incidents of CEF related incidents were reported in fiscal year 2023/24. During the period, 1,797 of such cases were investigated and closed and investigation is going on for 2,315 of the reported incidents. During the period case was filed for 25 cases related to CEF.

Cyber Bureau receives complaints and information related to CEF mainly from victims' complaints. In recent times, they have encountered several common typologies of cyber-enabled fraud (CEF). These include schemes such as offering online jobs, creating online learning platforms for language tests like IELTS, or sharing knowledge in various sectors. Fraudsters also lure victims by promising easy foreign visas or work opportunities, enticing them with lotteries, gifts like iPhones, or inheritance claims from wealthy individuals whose last names resemble the victim's, making them appear as likely heirs. Another common tactic involves scammers posing as staff from digital wallet companies, tricking victims into providing their OTPs by offering bonuses or gifts. Additionally, cybercriminals distribute malware, often in the form of batch files, to compromise victims' computers and laptops.

As per the Annual Report for the fiscal year 2022/23 issued by the Office of the Attorney General, a total of 29 fraud-related cases were registered at the Supreme Court of Nepal, of which 1 case resulted in a conviction, and 2 cases resulted in acquittals during the fiscal year. Furthermore, of the 495 fraud-related cases prosecuted before the High Courts, 153 cases resulted in convictions, while 163 cases resulted in acquittals.

The report further indicates that the District Government Attorney Offices registered 781 new fraud-related cases during the fiscal year, while a decision of non-prosecution was made in relation to 220 fraud-related cases. Additionally, a total of 1,898 fraud-related cases were before District Courts in the fiscal year 2022/23. Out of these cases, 300 resulted in convictions, 300 resulted in acquittals, and 225 cases were either withdrawn or adjourned.

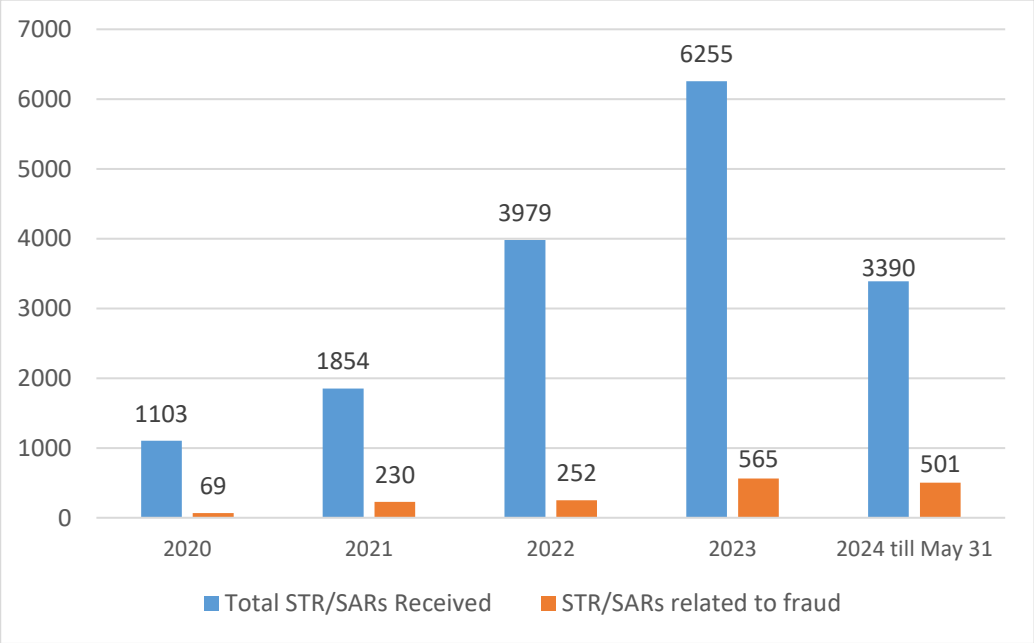
According to the Office of the Attorney General, in the fiscal year 2022/23, a total of seven cases concerning CEF were prosecuted, involving ten defendants. Of these cases, one resulted in a

conviction, partial claims were sustained in three cases, and one case was resolved through mutual compromise. Furthermore, one case was returned/postponed, and one case remains pending under the adjudication process.

2.4 Fraud related SARs/STRs and FIU-Nepal

REs are required to select at least one predicate offence while filing STR/SAR at FIU-Nepal. For purpose of this study, we have considered those STR/SARs in which at least one of the selected indicator was 'fraud'. Total STR/SARs received annually at FIU-Nepal and STR/SARs received with predicate offence 'fraud' is shown in the bar diagram below:

Figure 2-5 Fraud related STR/SARs received by FIU-Nepal



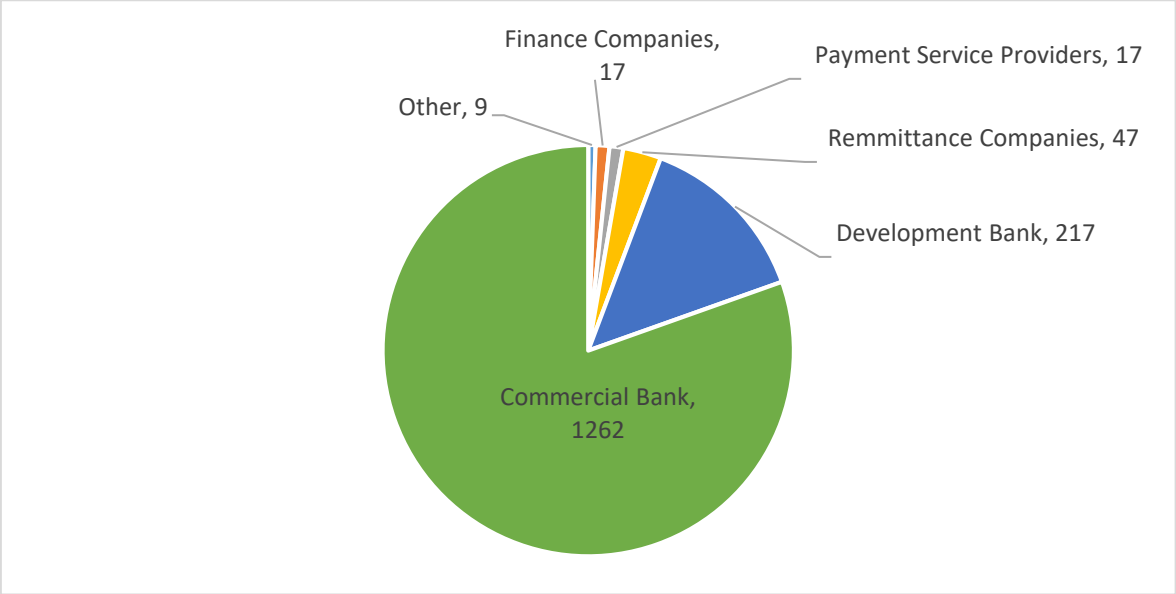
Total number of STR/SARs with indicator 'fraud' received from goAML web reporting and other medium during the period from Jan 1st, 2020 to May 31st, 2024 was 1569. Ratio of STR/SARs related to fraud were 6.33% and 9.03% of total STR/SARs received on year 2022 and 2023 respectively.

The ratio has increased to near 15% in first five months of 2024. Out of 3390 STR/SARs received from Jan 1st, 2024 to May 31st, 2024 number of STR/SARs related to fraud was 501. This shows that the proportion of reported suspicious transactions related to fraud with respect to total STR/SARs received in the year is in an increasing trend.

2.4.1 REs wise fraud related STR/SARs

Total number of fraud related STR/SARs received by FIU-Nepal during the period of Jan 1st, 2020 to May 31st, 2024 via goAML web reporting was 1569. Figure below presents REs wise reporting of fraud related STR/SARs.

Figure 2-6 Fraud related STR/SARs received from different REs



Among them, 1262 STR/SARs were received from commercial banks, 217 were received from development banks, 47 were received from remittance companies. PSPs and finance companies have reported 17 STR/SARs each, stock brokers and life insurance companies have reported 4 STR/SARs each while one cooperative organization has submitted fraud related STR/SAR using goAML web reporting.

2.4.2 Analysis and dissemination of STR/SARs related to fraud

Total number of suspicious transactions and activity reports analyzed, postponed and disseminated during the study period related to predicate offence 'fraud' is presented in table below.

Table 2-1 Number of STR/SARs analyzed, postponed and disseminated

Year	Analyzed	Postponed	Dissemination
2020	16	3	13
2021	89	22	67
2022	54	22	32
2023	155	91	64
2024 till May 31	97	51	37
Total	411	189	213

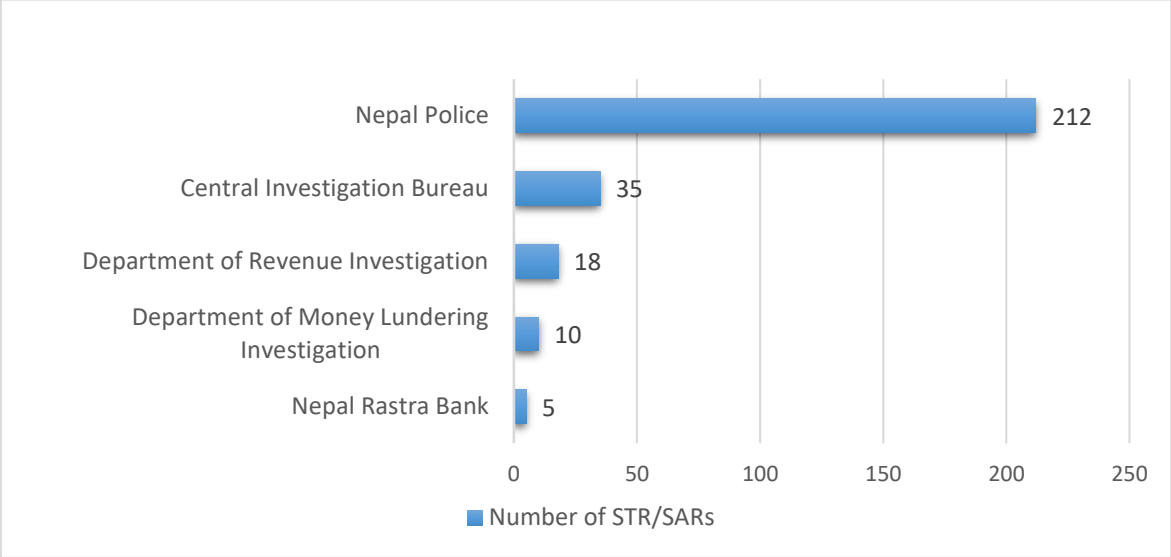
**The STR/SARs disseminated in a year may be received by FIU-Nepal in the previous year as well.*

Total number of fraud related STR/SARs analyzed from Jan 1st, 2020 till 31st May, 2024 was 411. Out of them 213 STR/SARs were disseminated to competent authorities while 189 STR/SARs were postponed.

2.4.3 Dissemination of fraud related STR/SARs to LEAs and investigative agencies

Of the 213 disseminations of fraud related STR/SARs mentioned in Table 2-1, number of STR/SARs disseminated to different LEAs and investigative agencies is shown in Figure 2-4 below. It should be noted that upon analysis each STR/SAR it can be disseminated to multiple agencies as per the nature of crime and its inter-connectedness.

Figure 2-7 Dissemination of fraud related STR/SARs to LEAs and investigative agencies



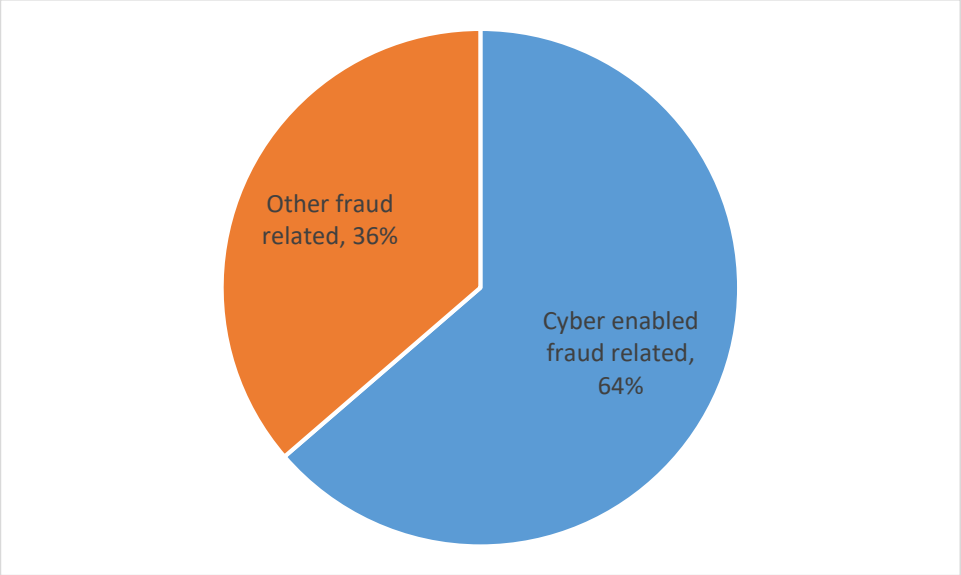
Note: FIU-Nepal can disseminate the analysis of same STR/SAR to multiple agencies based on involved predicate offence.

Fraud related cases are mainly investigated by Nepal Police. 212 of 213 such disseminated STR/STRs are disseminated to Nepal Police. Among 212 disseminations to Nepal Police, 166 STR/SARs were disseminated to Nepal Police only and remaining 46 were disseminated to other agencies as well along with Nepal Police. Dissemination of fraud related STR/SARs to Central Investigation Bureau (CIB), Department of Revenue Investigation (DRI), Department of Money Laundering Investigation (DMLI) and NRB was 35, 18, 10 and 5 respectively.

3. Analysis of CEF related STR/SARs received in year 2024

Proportion of fraud related STR/SARs received at FIU-Nepal was high in first five months of 2024 compared to previous years. To get the clear understanding of CEF, fraud related STR/SARs obtained in the same period i.e. 1st Jan to May 31st 2024 were studied. From them CEF related STR/SARs were separated and then studied in detail for further analysis of CEF. Among the 501 fraud related STR/SARs obtained during the period, 319 were found to be related to CEF. Remaining STR/SARs, which lacked elements of CEF, were mostly related to foreign employment, crypto currency and other virtual assets, online betting, remittance, check fraud, co-operative fraud and forgery.

Figure 3-1 Fraud related STR/SARs received in 2024 (till May 31st)

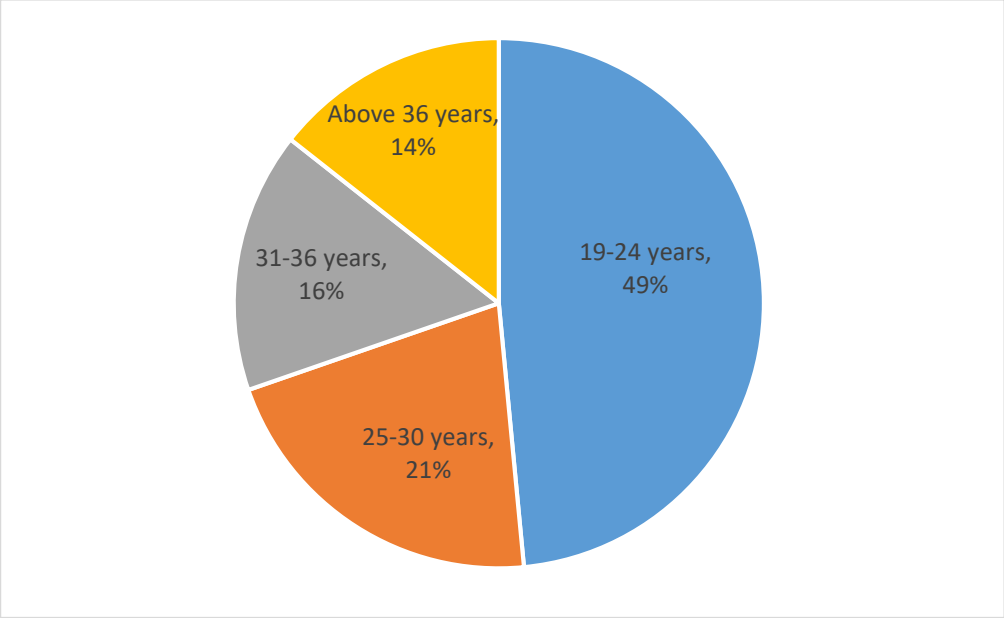


From among the 319 CEF related STR/SARs, a sample of 151 STR/SARs was selected on random basis for further analysis of CEF. Analysis was done in terms of age group and occupation of suspected persons, transaction behavior in suspected accounts, sources of STR/SARs generation, fraud typologies used, geographical location of suspicious accounts, tool used to contact the potential victim, factors influencing the reporting of SAR/STRs and other relevant data. The result of the analysis is presented in the section below.

3.1 Age group of the individuals reported in CEF related STR/SARs

Among the 151 STR/SARs in the sample, number of unique individuals whose STR/SAR was obtained was only 132. It was because STR/SARs were received from multiple REs for some of the individuals. The proportion of STR/SARs received for individuals under different age group is given in below figure.

Figure 3-2 Age group of individuals suspected of CEF

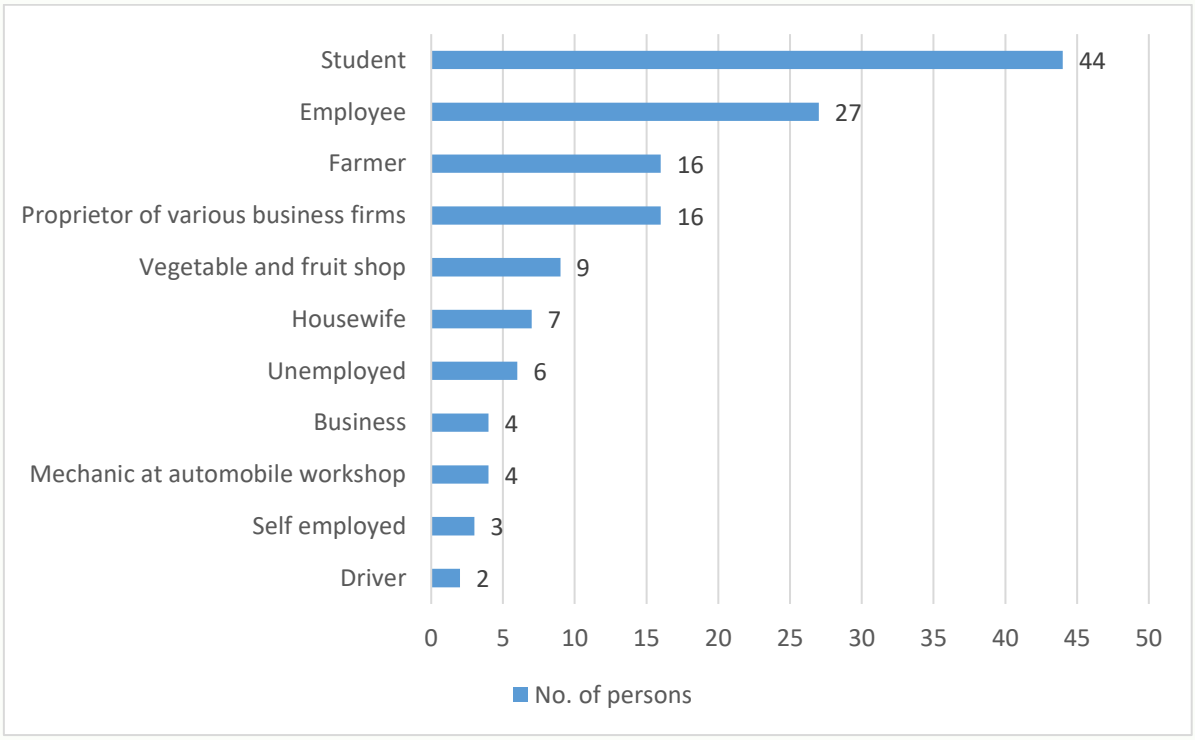


Of the individuals reported for suspicion of CEF 49% were in age group of 19-24 years and 21% were in age group of 25-30 years. i.e. 70% of the individuals suspected of CEF were of age group of 19 to 30 years.

3.2 Occupation of the individuals reported in CEF related STR/SARs

Among the 151 STR/SARs in the sample, occupation was mentioned in Know Your Customer (KYC) form of 138 suspected individuals only and it was not specified in remaining STR/SARs.

Figure 3-3 Occupation of individuals suspected of CEF



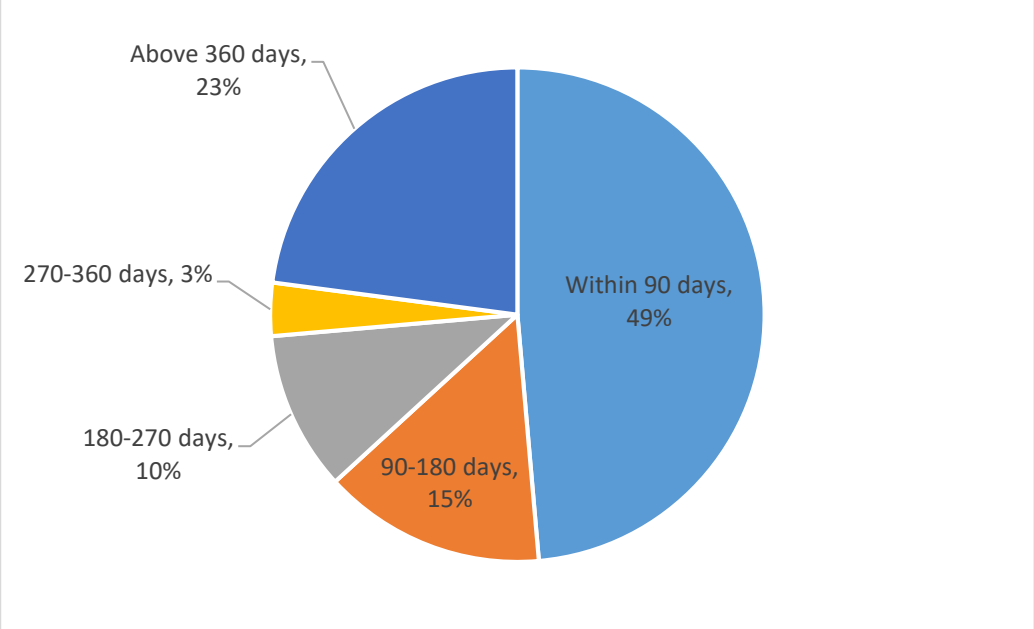
Among the individuals with occupation mentioned in KYC form, 44 had mentioned occupation as student. Similarly, 27 individuals mentioned their occupation as 'employee' of different organizations; 16 individuals mentioned farmer or agriculture; 16 individuals identified themselves as proprietor of various businesses like beauty parlor, fancy cloth store, metal workshop, electronic shop, kirana stores, café, restaurants, trading, construction sector etc. 9 individuals mentioned occupation as owner of small vegetable or fruit shop.

3.3 Account opening period and CEF related STR/SARs

Account detail of 145 accounts was available in the sample of 151 STR/SARs. Account detail is not applicable in STR/SARs received from some REs like remittance companies. Of the 145 accounts reported in the sample STR/SARs, seventy-eight percent of the accounts were found opened in 2023 and 2024 A.D. as shown in figure below.

Most of the STR/SARs related to CEF are seen reported for the accounts that were opened only few months before their STR/SAR was reported. Of the 145 suspicious accounts 49% were reported for CEF within 90 days of account opening. Similarly, other 25% of accounts were reported within next 90 -270 days of account opening. This shows that the fraudsters are continuously opening new accounts to carry out online fraud.

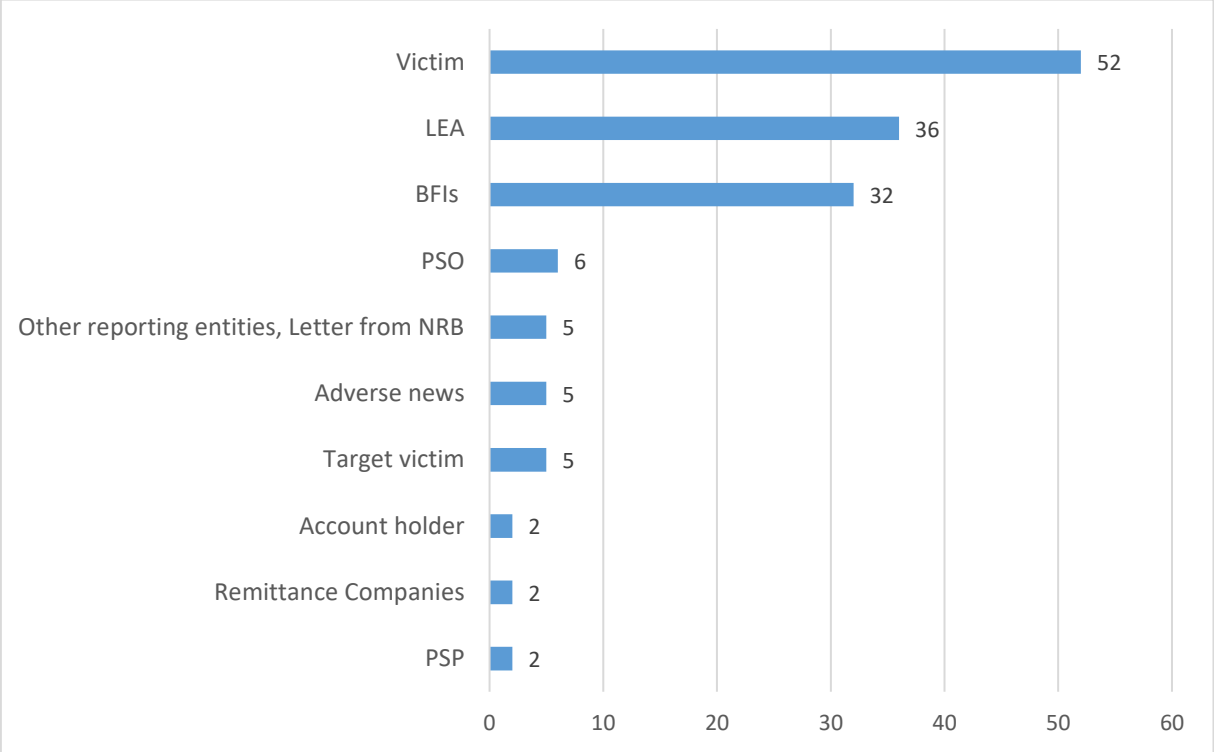
Figure 3-4 STR/SARs reported within certain days after account opening



3.4 Parties/sources affecting the generation of STR/SARs by REs

CEF related STR/SARs are mainly initiated by victims reporting or by monitoring mechanism of REs. The STR/SARs generated from REs may also be initiated after inquiry from LEAs and investigative agencies, adverse news, target victims and walk-in customers. Different parties and information sources triggering the REs for reporting of CEF related STR/SARs in the sample is given in Figure 3-5 below.

Figure 3-5 Source of STR/SAR and number of reported STR/SARs



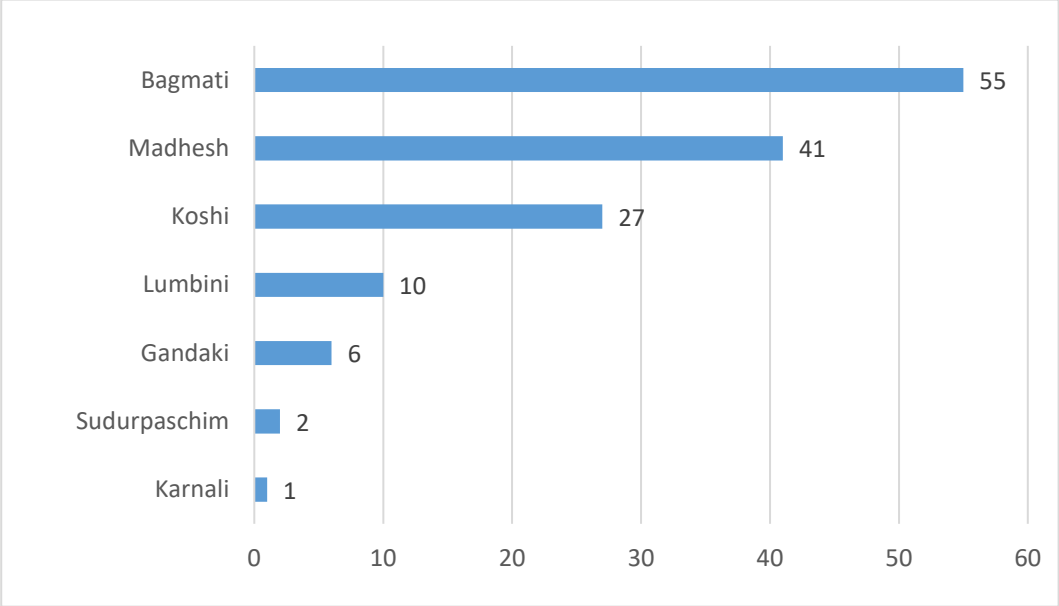
Highest number of STR/SARs in sample is seen initiated after victims reported the fraud to REs. The inquiry from LEAs accounted for second highest number of STR/SARs. These inquiries were also mainly initiated after victim reported the fraud incident to LEAs. It is seen that the LEAs have inquired about different persons/accounts involved in fraud after certain level of investigation of lodged complaint. BFIs and Payment Service Operators (PSOs) too have reported fraud related transactions through their regular account transactions monitoring. They have reported STR/SARs from the input from front office staffs and adverse news. STR/SARs were also initiated by BFIs after money mules account holders reported that their account was being misused. In the sample, only few STR/SARs were seen initiated by remittance companies and PSPs through their account monitoring mechanism.

3.5 Province wise accounts reported in CEF related STR/SARs

The 145 accounts studied in the sample are seen opened in different part of the countries as shown in figure below. Highest concentration of such account is seen in Bagmati Province followed by Madhesh Province. Third highest such accounts were opened in Koshi Province and fourth highest number of such account were seen opened in Lumbini Province.

Majority of accounts were seen opened in Kathmandu valley, Parsa, Dhanusha, Jhapa and Biratnagar district. In many cases accounts are seen opened in one place and operated from different place using digital medium and ATM transactions. In few cases it is also seen that cash withdrawal using physical ATM card is done in one place and card-less ATM cash withdrawal is seen in another geographical area of country. This indicates that the fraud network may be operating with physical presence across the country.

Figure 3-6 Number of accounts reported in CEF related STR/SARs

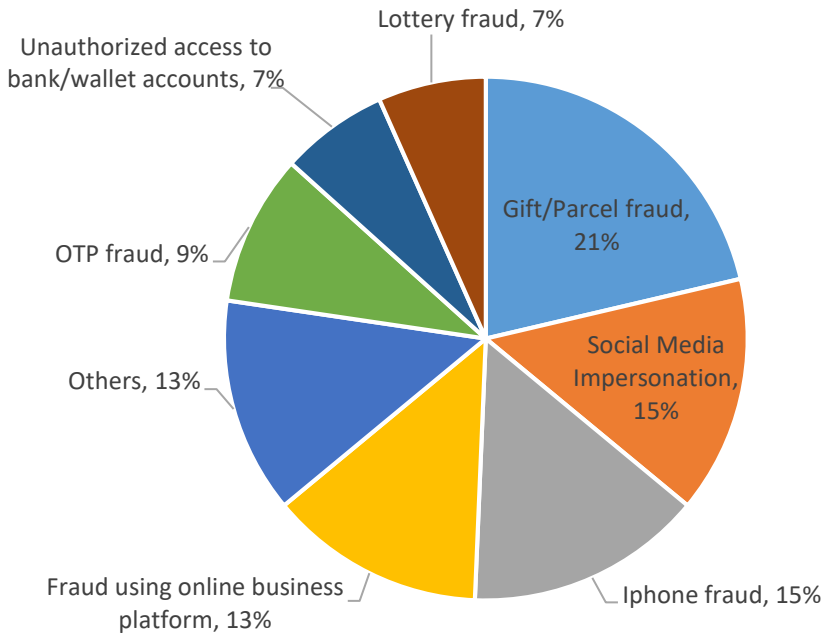


3.6 Typologies of CEF identified in STR/SARs

The content in reason field of STR/SARs, keyword used by REs as well as attachments provided were studied to identify typology of CEF used in STR/SARs. Identifying the typology of CEF was more straightforward in STR/SARs where reporting entities included the victim's complaint. It also became easier when the REs clearly noted the verbal complaint of the victim in the remarks section of STR/SARs. It was difficult to identify typology used in STR/SARs where REs did not provide sufficient information.

The typologies of CEF used, based on the identified typologies in the sample of STR/SARs, are shown in figure below.

Figure 3-7 Number of STR/SARs reported indicating different CEF typologies



Fraud by tempting free gift/parcel was most reported CEF typology in the sample. Fraud using social media impersonation and fraud by tempting victims to free Iphone and apple products were jointly second highest reported typology. Social media impersonation was mainly seen in Whatsapp and Facebook accounts. Hacking of Facebook account was frequently linked to social media impersonation in Facebook. The frequent reporting of social media impersonation involving the use of photos and names of prominent public figures was also noted. Fraudsters used these fake Facebook accounts to chat with the close relatives and friends of real persons and asked for money from them by using various tactics, including creation of fake emergency.

Fraud by creating fake online business/trading platform was third highest reported CEF typology followed by fraud by tricking victims into sharing OTP for banking transactions. Fraud using fake lottery and debit of fund by unauthorized access to bank/wallet accounts were among common CEF typologies. Fraud using various schemes like money double, investment in cryptocurrency, network marketing, online room rent service, online examination fee for PTE & IELTS etc. were among other CEF typologies reported at FIU-Nepal.

3.7 Other observations in CEF related STR/SARs:

- In earlier STR/SARs fraudsters have used Imo Chat and Facebook to contact victims. In recent days victims are mainly contacted by facebook messenger, Whatsapp, Tiktok, Instagram and other new social media.
- Fraud amount is debited by cash withdrawal using ATM card or via fund transfer to different bank and wallet accounts. In most of the cases place of cash withdrawal different from place of account opening. ATM withdrawal and POS transactions are also done from different cities in India. Of the transactions in India, repeat cash withdrawal using ATM are seen in same area, and even many ATM cards are used for POS transactions in same merchant.
- STR/SARs of same person is obtained from multiple REs. Multiple reporting in more evident in cases where LEAs have issued letter for investigation to multiple REs. However, some BFIs have now started sending CEF related STR/SARs only after getting some added information to such letters.
- Persons reported for CEF have opened accounts in multiple banks and financial institutions, and digital wallets within a period of few days in many reported cases. In few cases, fraudsters have opened money mule accounts with stolen identities, and by manipulating citizenship and other identity cards.
- Regular small value debit transactions is seen in accounts reported for CEF. The purpose of such transactions is to check if account is frozen by REs. If the account is found frozen, fraudsters change the destination account used to collect fraud money.
- The suspicious accounts reported for being used to carryout online fraud are also seen associated with online betting and crypto currency related transactions.
- Large number of digital transactions involving ConnectIPS, different wallet accounts and Fonepay account transfer are seen in the accounts of illiterate persons who seem to be incapable of such digital payment methods. On scrutiny, these accounts seem to be operated by the fraudsters as money mule accounts.

4. Findings and Recommendation

4.1 Key Findings

- Fraud related STR/SARs are in increasing trend with respect to total STR/SARs. Around 15% of the STR/SARs received in 2024 (till 31st May) were related to predicate offence 'fraud'. Similarly, portion of CEF related STR/SARs with respect to total fraud related STR/SARs received in 2024 (till 31st May) was above 63% indicating rising CEF incidents in Nepal.
- Majority of fraud related STR/SARs are disseminated to Nepal Police and Central Investigation Bureau (CIB), followed by Department of Revenue Investigation (DRI) and Department of Money Laundering Investigation (DMLI).
- Commercial banks and development banks have reported major portion of CEF related STR/SARs. Although digital wallets are frequently used for CEF, only few STR/SARs related to CEF are reported from PSPs.
- Age group 19-24 people are mostly suspected of CEF in reported STR/SARs followed by age group 25-30 years. In total 70% of the individuals suspected of CEF were in age group 19-30 years. This indicates most people involved in CEF directly, or indirectly as money mules, are people in age group 19-30 years.
- Occupation was mentioned as 'student' in largest number of accounts that were reported for CEF, followed by 'employee' of various organization. Similarly, other significant occupations mentioned in accounts reported for such fraud were 'farmer', 'proprietor', 'vegetable and fruit shop', 'housewife', 'unemployed'.
- Nearly half of the accounts linked to CEF were reported within three months of account opening. Similarly, around three fourth of the accounts were reported within nine months of account opening, suggesting use of new accounts for collection of proceeds of fraud.
- The main trigger for CEF related STR/SARs generation from REs was reporting by the victim to REs. Inquiry from law enforcement and investigative agencies was another significant reason for STR/SARs reporting. Similarly, transactions monitoring by BFIs and PSOs, adverse news, walk-in customers and letter from regulators like Nepal Rastra Bank were other factors contributing for initiation of STR/SARs.
- Province wise, highest number of accounts reported for CEF were opened at Bagmati province followed by Madhesh and Koshi province.
- Major typologies used in CEF are gift/parcel fraud, social media impersonation, iPhone fraud, fraud using fake online business platform, OTP fraud, lottery fraud and access to bank/wallet accounts using various fraudulent techniques. Money double scheme, investment in cryptocurrency, network marketing, online room rent service, online examination fee for PTE & IELTS etc. were among other CEF typologies reported at FIU-Nepal.
- Fraudsters contact victims initially via social media and then use other medium as the plot for fraud develops. The use of media to contact victims and techniques to defraud are constantly evolving.
- The fraud amount collected from unsuspecting victims is immediately withdrawn using ATM from different parts of country and India, or is transferred to other bank accounts and wallet accounts.
- Fraudsters have opened accounts in multiple BFIs and PSPs using same credentials, in a short period. Same mobile numbers are used to open these multiple accounts. Although KYC of such

account holders suggests they are incapable of performing digital transactions, frequent digital transactions per day are seen in these accounts.

- Frequent debit amount of as low as Re. 1 is observed in most of the accounts reported for CEF. Such amount is credited in various wallet accounts opened from frew common mobile number.

4.2 Recommendations

4.2.1 Recommendations to REs (BFIs and payment systems industry)

REs can adopt below mentioned practices for countering CEF, based on findings of this report and anti-fraud measures adopted by REs alongside AML/CFT controls across different countries. These measures also focus on customer verification and transaction monitoring for better anti-fraud control in payment industry.

- Implement robust Know-Your-Customer (KYC) including biometric features during onboarding of customers who use digital banking products. Checking whether mobile number used to access mobile/internet banking and wallet account is registered in customer's own name or immediate family member name or not.
- Implement the use of multi-factor authentication methods like e-mail, text OTP in registered mobile number, biometric verification, authenticator app etc. in order to verify customers and conduct financial transactions above certain threshold. Adopt enhanced measures to mitigate risk when customer adds new devices to conduct transactions.
- Implement provision of certain cooling-off period for digital banking transactions for new account opening or during the first-time enrolment to service. This may include limiting the number and value of transactions and limiting the number of devices to access digital banking products.
- Implement risk-based real-time transactions monitoring system, robustness of which is based on the volume and nature of transactions handled by REs. Implement tight fraud detection rule and triggers based on number and value of transactions, login times, transaction patterns, device usage, geolocation, counterparty, remarks etc. to proactively detect and report fraud transactions.
- Limit social media and email communication for general information only. Explicitly remind customers that identification detail, personal data and account detail should not be shared in these communication mediums.
- Educating customers about safe online banking practices. Provide guidance to customers regarding phishing attempts, passwords safety, possible data breach while using of public Wi-Fi for banking transactions.
- Educating employees about cyber-security best practices to mitigate insider threats. Conduct regular training sessions on topics such as recognizing phishing attempts, secure handling of sensitive information, and the importance of following security protocols. Due to continuous change in modus operandi of CEFs, strengthen capabilities of compliance staffs by providing regular training, enabling them to screen and categorize incoming STR/SARs relating to CEF.

4.2.2 Recommendation to LEAs and investigative agencies

Domestic co-ordination and co-operation is required between multiple agencies and private sector entities to implement strategies needed to identify, investigate and prevent CEF and related money

laundering. LEAs and investigative agencies can implement below mentioned measures for this purpose.

- Identify competent authorities and clearly assign responsibility for handling CEF cases to avoid duplication and improve consolidation of investigations involving multiple victims of similar fraud.
- Consolidate all CEF cases under one enforcement unit to improve data analytics, identify criminal syndicates, and serve as a single point of contact for private sector collaboration, with proper resource allocation for financial investigations and intelligence. Work closely with private sector entities to ensure timely access to financial information, enabling faster investigations and tracing of CEF proceeds.
- Launch educational campaigns targeting both the public and financial sector personnel to increase awareness of evolving CEF trends, improving detection and reporting of such crimes. Identify potential money mules based on reported cases, and dissuade them through public education and outreach.
- Develop platforms to facilitate rapid tracing and information exchange across different financial institutions to intercept illicit proceeds. Establish central registers or databases for fraud incidents to streamline information retrieval, enabling law enforcement to focus investigations on relevant financial institutions, identify money laundering networks, prevent fraud, and enhance asset recovery.
- Eliminate the tools and methods that facilitate fraud by deactivating mobile numbers, phone lines, and fraudulent websites used by criminals; implement filters for phishing messages and malicious links; and remove suspicious social media accounts, advertisements, and fraudulent apps.

4.2.3 Recommendations to regulators/supervisors

- Educate the public and increase vigilance against CEF. Implementing national awareness campaigns promoting cyber literacy and encouraging victim reporting.
- Encourage financial institution to adopt transaction monitoring to identify, prevent and report fraudulent activities in real-time. Keep newly opened accounts under increased monitoring as per the KYC profile and profession of account holders.
- Support stakeholders in leveraging informal channels to gather and secure intelligence quickly. Formal co-operation can be used later to obtain the necessary evidence and statements for preparation of judicial proceedings.
- Make financial institutions and payment systems providers liable in cases where lapses in their platform, mainly due to negligence in KYC requirement, has enabled scammers to carry out fraud.
- Encourage wallet insurance and card insurance to protect people who are unaware of digital frauds, and people who genuinely get defrauded. For example, eSewa has introduced wallet insurance, which covers losses arising from unauthorized transaction.

Annex I: Red flags for REs for CEFs

Following are the risk indicators that aim to enhance the detection of STR/SAR related to CEF. The presence of any one or more of these indicators in relation to a customer or transaction may not necessarily lead a clear indication of a cyber-enabled fraud offence. However, it could prompt further monitoring and examination of these transactions.

Transaction patterns

- Frequent or immediate transactions after opening of an account, inconsistent with the purpose of the account. Abnormal transaction activity in bank account and wallets including transaction with persons suspected of online gambling and illegal virtual assets transactions.
- Immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer keeping the balance in account near nil.
- Frequent and large transactions, which are inconsistent with the account holder's economic profile (e.g., sudden international transfers, withdrawals of cash performed through cards at bordering cities in India).
- Digital transactions being performed frequently in accounts related to illiterate persons or to persons with low knowledge of such digital payment methods.
- Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary
- Regular small value debit transactions to check if account is frozen so that the destination account of the funds can be changed if the account is frozen. Loading up of common wallet accounts or topping up of common mobile numbers from different accounts.
- Reaching maximum ATM cash withdrawal limit on a card on regular basis.
- The user is seen accompanied by an individual (by being physically present or over phone) during transaction as observed by bank staffs or through Closed Circuit Television (CCTV).

Customer transaction remarks

- Transaction remarks for account transfer contains a different language, timing, and amounts than previous transaction instructions. The instructions may include language that suggest transaction to be urgent and confidential.
- A customer presents poorly formatted messages / emails with spelling and/or grammar mistakes as justification of a transaction.
- The beneficiary's account information is different from what was previously used. The intended beneficiary in the transaction description and the name of the account holder at beneficiary bank are inconsistent
- Repeated transaction with same remarks such as Payment, Borrowings etc.

Suspicion in account holder's profile and behavior

- REs may be unable to contact account holder or face non co-operation from account holder for Customer Due Diligence (CDD).
- Account holders accompanied and assisted by unrelated persons during account opening. Such account holder may be unaware of the source of funds or pretend to be working on behalf of someone else.

- The customer shows inadequate knowledge on the nature, amount or purpose of the transactions. Customer provides non-realistic and inconsistent explanations to the transaction creating suspicion that the customer is acting as a mule.
- Seemingly illiterate person subscribing to latest digital payment products like mobile banking, internet banking, connectIPS, wallets etc.
- Customer is completely unware of the transaction purpose.

Suspicion in account holder's identity

- The account holders' attempts to hide their identity by using shared, falsified, stolen or altered identification (address, telephone number, email). The phone numbers provided during account opening are unreachable.
- E-mail addresses seem to be incompatible with the name of the account holder and seem more like of other person's e-mail. Similar email addresses pattern seen across multiple accounts. Same mobile number and e-mail addresses and other credentials shared by two or more account holders.
- IP addresses or GPS coordinates originating from other jurisdictions; use of Virtual Private Networks (VPNs) to mask a user's IP address; multiple IP addresses or electronic devices associated with a single online account; single static IP address or electronic device associated with multiple accounts of various account holders.
- User audit trail suggesting multiple failed transactions attempt before successful transactions and multiple successful transactions followed by a successful transaction.

Adverse information on the account holder

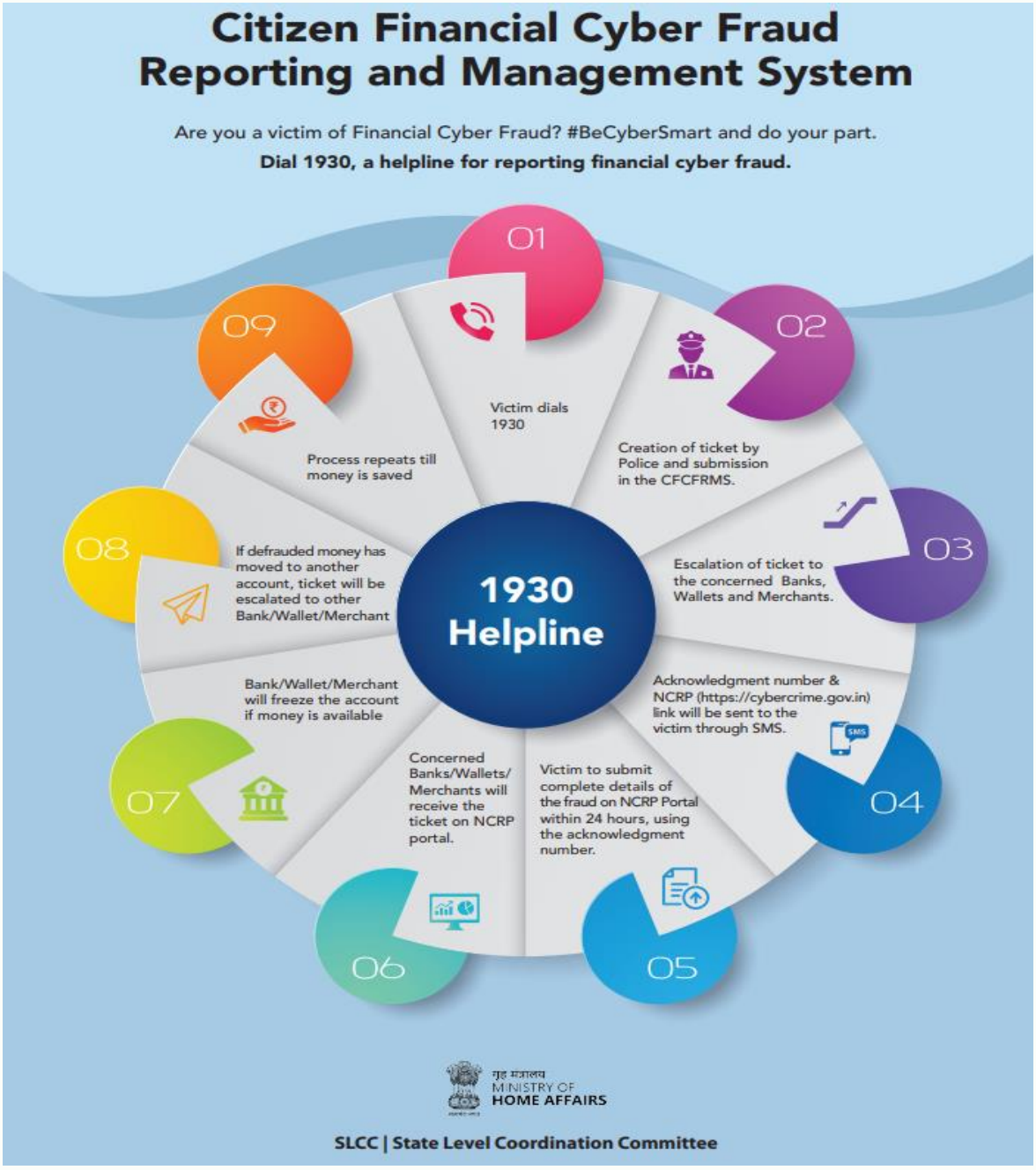
- Presence of adverse news on customer or counterparties, e.g., account held by a previously known suspect of scam, money mule, or identity takeover activity.
- Fraud report or wire transfers' recall requests from a correspondence institution.
- Presence of adverse information provided by FIUs or LEAs about persons involved in a transaction.

Annex II: Notable international practices to counter CEF

Below presented are some of the notable practices adopted by different jurisdictions and organizations to counter CEF. These practices are highlighted in different publications of FATF, APG, FIUs' of different jurisdictions and other organizations in the field of cyber security.

(A) India: Some efforts in India to curb CEF.

Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)



Source: Puducherry (py.gov.in)

The CFCFRMS is an online system developed by the Indian Cyber Crime Coordination Centre for quick reporting of financial cyber frauds and preventing the flow of fraud proceeds across the financial sectors. The system has integrated LEAs across the country and financial entities (i.e., bank, wallets, payment aggregators, payment gateways, e-commerce platforms etc.) together

to work in tandem and take immediate action on the complaints reported on CFCFRMS. At present all State and Union Territory LEAs and 243 Financial Entities are onboarded on the module. Once a victim reports a fraud to the LEA, details of the beneficiary of the fraudulent transaction is recorded and submitted to the CFCFRMS system in a form of a ticket. This ticket is escalated to the concerned financial entity (bank, payment wallet etc.), which will see the ticket on its system's dashboard. The Entity will check if the defrauded funds are still in the account and puts it on hold. If the funds have been dissipated to another entity, the ticket is escalated to that next entity-layer. The process is repeated until the money is intercepted. If the money is withdrawn, the details of withdrawal are filled by FIs for further action of LEAs. The system has been highly effective in preventing fraudulent transactions from going into the hands of fraudsters. More than 10.10 lakh incidents for financial fraud have been registered on CFCFRMS from 01.01.2023 to 30.11.2023.

(See more at https://pib.gov.in/PressReleasePage.aspx?PRID=1988272)

Digital India Trust Agency to check illegal loan apps.

The Reserve Bank of India (RBI) is considering a new weapon in the fight against cybercrime, the Digital India Trust Agency (DIGITA). This proposed agency would target the rise of illegal loan apps by verifying legitimate ones and creating a public registry. DIGITA would act as a central hub for vetting digital loan apps. This verification process would ensure apps comply with regulations and operate ethically. Only verified apps would receive a "DIGITA-approved" seal, making them easily identifiable for borrowers. Apps without DIGITA's verification may be penalized. Sources suggest that law enforcement might consider them unauthorized. This would be a major step towards combating financial scams and protecting borrowers in the digital lending space.

(See more at: http://timesofindia.indiatimes.com/articleshow/108958433.cms?utm_source=_contentofinterest&utm_medium=text&utm_campaign=cppst)

Cyber Swachhta Kendra

The 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. It is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco-system in the country. This center operates in close coordination and collaboration with Internet Service Providers (ISPs) and product/antivirus companies. This website provides information and tools to users to secure their systems/devices. The Indian Computer Emergency Response Team (CERT-In) is operating this center.

(See more at https://www.csk.gov.in/)

(B) Sri Lanka: Rapid Actions to Prevent Scams (RAPS) project

FIU Sri Lanka has launched a project, called Rapid Actions to Prevent Scams (RAPS), to act immediately once a victim reports potential CEF. The objective is to disrupt scams in the Sri Lankan financial system, including CEF, by bringing together the FIU and compliance officers of the FIs to rapidly detect illicit account activities used by criminals and their accomplices. The mechanism involves identifying the credentials of the scammers based on the public complaints

received, and the credentials of such fraudsters are shared with the compliance officers of the FIs. Based on this information, the FIs monitor the account activities of potential fraudsters and take appropriate actions to disrupt the use of the financial system to prevent any fraud. Additionally, the fraudsters' information is shared with Sri Lanka Police to conduct investigations on the subjects.

See more at: Illicit Financial Flows from Cyber-enabled Fraud (fatf-gafi.org) p. 37

(C) China: Co-operation with telecommunications sector

China has continued to promote the strengthening of combating and managing telecommunications network fraud. On December 1, 2022 China officially implemented the 'Anti-Telecommunication Network Fraud Law of the People's Republic of China', which has provided strong rule of law safeguards to combat and curb criminal activities of telecommunications network fraud, and related criminal acts have been effectively curbed. The law requires telecom operators, financial institutions and ISPs to set up internal systems for controlling fraud risks. The law brings together public sector authorities (including law enforcement, financial, telecommunications and internet information agencies), as well as FIs (banks and non-bank payment service providers), telecommunications business operators and ISPs to establish an early warning and dissuasion system. This system identifies potential victims by providing an early warning, allowing appropriate and timely dissuasive measures to be taken. FIs can also use this system when opening bank accounts, payment accounts, and provide payment and settlement services. The system is used to enhance customer due diligence processes and allows the FIs to take risk mitigation measures to prevent bank and payment accounts etc. to be used for fraudulent activities.

(See more at:http://en.moj.gov.cn/202312/15/c_948363.htm#:~:text=Article%2046%20Offenders%20and%20criminals,of%20the%20People%27s%20Republic%20of)

(D) Singapore: Anti Scam Command (ASCom)

The Anti-Scam Command (ASCom) was operationalized on 22 March, 2022 to achieve greater synergy between various scam-fighting units within the Singapore Police Force (SPF), by integrating scam investigation, incident response, intervention and enforcement under a single umbrella. The command comprises the Anti-Scam Centre, three Anti-Scam Investigation Branches, and oversees the Scam Strike Teams situated within each of the seven Police Land Divisions. The ASCom focuses on upstream interventions to disrupt scammers' operations and leverages technology to strengthen its sense-making capabilities. The ASCom partners with more than eighty institutions in the fight against scams. These include local and foreign banks, card security groups, non-bank financial institutions, Fintech companies and cryptocurrency houses and remittance service providers in Singapore. Through establishing direct communications channels and close working relationships, the ASCom and its partners seeks to swiftly freeze accounts, recover funds and reduce losses suffered by victims. As part of the continued collaboration in combating scams, the ASCom and the Monetary Authority of Singapore worked with the banks to co-locate their staff within ASCom premises to enhance real-time coordination with the police in investigative efforts, tracing the flow of funds, and freezing bank accounts suspected to be involved in scam operations. In addition, the Government Technology Agency has deployed staff at the ASCom to support police

investigations in scams related to Singpass (Singpass stands for Singapore Personal Access, a digital identity to access government agencies and businesses). ASCom also will works closely with foreign law enforcement counterparts to detect and tackle emerging crime trends. The ASCom works with relevant units in the police to target persons who facilitate scam-related activities, for example, money mules who assist in bank transfers, relinquish bank accounts and disclose Singpass and internet-banking credentials to the scammers. Through the close collaboration with the newly set-up Scam Strike Teams in the seven land divisions, the ASCom is dedicated to taking swifter and more holistic actions to tackle scam cases that are currently plaguing Singapore and the world.

(See more at: https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scamcommand_of fice)

(E) United Kingdom: Action Fraud

The Action Fraud is the United Kingdom's national report center for fraud and cybercrime. It is national reporting center for fraud and cyber-crime where persons who are scammed, defrauded or have experienced cyber-crime. It provides a central point of contact for fraud and financially motivated internet crime and is run by the City of London Police, alongside with the National Fraud Intelligence Bureau (NFIB). The Action Fraud website provides various public outreach resources for crime prevention as well as victim protection and support. The Action Fraud also runs an online 24/7 live reporting portal for victims. Action Fraud reports are passed to the NFIB, who assesses and analyses across different parts of the country to identify the ultimate perpetrators. These reports are then sent to the appropriate local police forces within the United Kingdom for investigations. The NFIB also uses these reports to take down bank accounts, websites and phone numbers used by fraudsters.

See more at : https://www.actionfraud.police.uk/

(F) Australia: Joint Policing Cybercrime Co-ordination Centre (JPC3) and Operation DOLOS

Joint Policing Cybercrime Co-ordination Centre (JPC3)

The Australian Federal Police (AFP) leads the Joint Policing Cybercrime Coordination Centre (JPC3). Membership of the JPC3 includes federal and state law enforcement, government analysts including AUSTRAC, and industry partners, such as analysts from Australian banks. The JPC3:

- Coordinates Australia's policing response to high harm high volume cybercrime to maximize impact on the criminal environment;
- Enhances intelligence sharing and target development across Commonwealth, State and Territory police and industry;
- Coordinates joint taskforces with police and industry partners to counter priority cybercrime threats;
- Provides national coordination to uplift capability via skill sharing, joint training and collaborative tool development; and
- Communicates nationally consistent prevention, awareness raising and media activities to industry and the public.

The JPC3 has a prevention capability that works with industry and the public domain on combatting cybercrime. To effectively support the JPC3, AUSTRAC also has a financial cybercrime team, which specifically focus on providing financial intelligence regarding cyber-enabled and cyber-dependent crime with a financial nexus, which includes ML of CEF.

Operation DOLOS

In January 2020, the AFP established Operation DOLOS which, is an AFP led, multi-agency taskforce which counters transnational cybercriminals conducting or facilitating Business Email Compromise (BEC). Operation DOLOS works with individual Australians and small to medium businesses that have been targeted by BEC and disrupts the flow of proceeds to and from BEC syndicates. Since the commencement of Operation DOLOS, the taskforce developed new techniques leading to reduced harm to Australians and enterprises. Between 1 July 2022 and 30 June 2023, Operation DOLOS has prevented more than AUD30.6million from being lost from Australian and international victims by disrupting the financial operating model used by criminals.

See more at : Illicit Financial Flows from Cyber-enabled Fraud (fatf-gafi.org) p. 36-37

(G) Hong Kong: e-Crime Processing and Analysis Hub (e-Hub) for using technology to delineate investigative responsibility

The Hong Kong Police Force (HKPF) established the e-Crime Processing and Analysis Hub (e-Hub) in September 2022 with the aim of enhancing the efficacy in handling technology crime and deception-related reports. The e-Hub uses enhanced computer system to perform correlation analysis against common types of CEF cases and identifies case clusters. In 2022, the number of deception cases increased by 45.1% to 27,923 cases, accounting for almost 40% of the overall number of crimes. Nearly 80% of the deception cases were CEF related. More people are reporting CEF online and most of the e-reported cases are correlated, such as from the same criminal group. The correlated cases are assigned to one single investigation team for consolidated investigation so that resources could be better coordinated. By using clustering algorithms, e-HUB can identify patterns and similarities in the data that might not be immediately apparent to gain a deeper understanding of the scope and nature of cases. This includes common types of criminal digital tools and money mules accounts used, and how CEF is planned, executed, and concealed.

See more at: https://www.police.gov.hk/offbeat/1219/eng/9001.html

(H) Malaysia: National Scam Response Centre (NSRC)

Malaysia's National Scam Response Centre (NSRC) is a multi-faceted response center that brings together a diverse range of resources and expertise from the National Anti-Financial Crime Centre, Royal Malaysia Police (RMP), the Central Bank and other public and private sector entities. The NSRC serves as a hub for fraud information received from various sources and leverages network analysis to identify mule and laundering networks. Private sector entities, including financial institutions, will trace the funds from one layer to another layer and subsequently withhold the mule accounts. The RMP will further investigate the case and take enforcement action such as issuing freezing order to the accounts.

See more at: https://nfcc.jpm.gov.my/index.php/en/faq/about-nsrc

(I) Brazil: Centralized private-private database

Brazil has recently approved a Resolution making mandatory a database that centralizes information regarding fraud (including attempts) by all financial and payment institutions. Banco Central do Brazil (BCB) issued the resolution on 4 October 2023 to outline procedures for sharing data on fraud, as mandated by the Resolution. The Resolution institutes that sharing information about frauds (including attempts) are compulsory for institutions and defines minimum information that must be shared. This includes identification of the persons involved in the commitment of fraud (including money mules), the financial institution(s) involved, and the account(s) used. The system aims to facilitate information sharing between private sector, with the objective to prevent and combat fraud, as well as recover illicit fraud proceeds.

See more at: https://www.lexology.com/library/detail.aspx?g=d774b647-949e-48c0-85ec-ddf71eeb6d12

(J) Saudi Arabia: Joint Operations Room (JOR)

Saudi Arabia established a Joint Operations Room (JOR) for banks. The JOR is tasked with following up and monitoring cases of financial fraud that bank customers may be exposed to. The JOR brings together all banks and related financial institutions under one umbrella to tackle confirmed cases of financial fraud. The JOR is hosted by banks in Saudi Arabia to facilitate join efforts for the stability of the banking sector. The JOR operates 24/7 and aims to provide quick and effective co-operation and integration between all Saudi banks to limit the development of fraud cases, as well as to provide a swift response to fraud complaints and where possible to take immediate actions to avoid fraudulent acts.

See more at https://www.spa.gov.sa/2371915

(K) World Economic Forum: Partnership against Cybercrime

The Partnership against Cybercrime (PAC) project is part of the World Economic Forum's 'Centre for Cybersecurity' which was launched in 2020 to promote public-private cooperation to combat cybercrime. It serves as a platform for insight sharing and continuous exploration of approaches to drive successful collaboration against cybercrime.

The PAC brings together a dedicated community of global businesses, leading national and international LEAs, and leading not-for-profit organisations. The PAC aims to shift the balance between cybercriminals and defenders by mobilizing the private sector and promoting public-private cooperation.

(See more at : https://www.weforum.org/projects/partnership-against-cybercime/)

Annex III: Public awareness messages issued by different entities

(A) Public notices issued by Payment Systems Department (PSD) of Nepal Rastra Bank:

नेपाल राष्ट्र बैंक
भुक्तानी प्रणाली विभाग

विद्युतीय माध्यमबाट वित्तीय कारोबार गर्दा हुनसक्ने जोखिमका सम्बन्धमा सर्वसाधारणका लागि जारी गरिएको सूचना

नेपालमा पछिल्लो समयमा विद्युतीय कारोबारमा बढोत्तरी भइरहेको छ । विभिन्न विद्युतीय उपकरणको माध्यमबाट घरमै बसेर कारोबार गर्दा विभिन्न आपराधिक व्यक्ति/समूहले विभिन्न माध्यम प्रयोग गरी ग्राहकलाई ठगी गरिरहेको भन्ने गुनासो प्राप्त भइरहेकाले देहायका विषयमा विशेष ध्यान दिन नेपाल राष्ट्र बैंक विद्युतीय भुक्तानी प्रयोगकर्तामा विशेष आग्रह गर्दछ :

१. सामाजिक सञ्जालमार्फत चिनजानका मान्छेको नाममा रकम माग गर्ने, बैंकबाट फोन गरेको भनी Internet Banking अथवा Mobile Banking को User Name तथा Password माग्ने, नक्कली Website बनाई ग्राहकका गोप्य सूचनाहरू लिने, ठूलो रकमको चिट्ठा परेको भनी लोभ देखाई उक्त चिट्ठा रकम हस्तान्तरण गर्ने बहानामा रकम माग गर्ने, अत्यधिक नाफाको लोभ देखाई गैरकानुनी घोषणा गरिएका उपकरणमा लगानी गर्न उत्प्रेरित गर्नेलगायतका ठगी भइरहेको जानकारीमा आएकोले विद्युतीय कारोबार गर्दा यसप्रकारको ठगीबाट बच्न विशेष ध्यान दिनु जरुरी देखिन्छ ।

२. अपरिचित व्यक्तिलाई कुनै पनि माध्यमबाट आफ्नो गोप्य Password, OTP वा अन्य कुनै पनि संवेदनशील जानकारी दिनुहुँदैन । मोबाइल तथा अन्य डिभाइस एवम् APP का पासवर्डहरू बेलाबेलामा परिवर्तन गर्नुपर्दछ । यस्ता पासवर्ड गोप्य तरिकाले सुरक्षित राख्नुपर्दछ ।

३. सामाजिक सञ्जाल वा कुनै विद्युतीय माध्यमबाट म्यासेज पठाई रकम पठाउन आग्रह गरेमा रकम पठाउनुअघि सोही व्यक्तिले रकम माग गरे नगरेको व्यहोरा अन्य माध्यमबाट यकीन गरेर मात्र रकम पठाउनु पर्दछ ।

४. अनावश्यक तथा अनधिकृत APP आफ्नो मोबाइल फोन वा अन्य डिभाइसमा डाउनलोड गर्नुहुँदैन । यसरी अनधिकृत APP डाउनलोड गर्दा आफ्ना सबै संवेदनशील सूचनाहरू आपराधिक समूहले पत्ता लगाउन सक्छन् ।

५. कसैले रकम भुक्तानी गर्ने बहानामा Barcode अथवा QR Code पठाएको अथवा APP को पासवर्ड आवश्यक छ भनेर म्यासेज गरेको कार्यलाई शङ्कास्पद रुपमा लिनुपर्दछ । रकम भुक्तानी लिन वा पैसा प्राप्त गर्न कुनै पनि Barcode, QR code अथवा पासवर्ड पठाउन आवश्यक छैन ।

६. कुनै पनि Website मार्फत विद्युतीय कारोबार गर्नुअघि सम्बन्धित संस्थाको आधिकारिक Website हो/होइन यकीन गरेर मात्र कारोबार गर्नुपर्दछ । कुनै पनि Website को ठेगाना "https://" बाट सुरु भएको छ भने सुरक्षित, भरपर्दो वा विश्वसनीय छ भन्ने बुझिने भएकोले Website को ठेगाना "https://" बाट सुरु भए नभएको यकीन गर्नुपर्दछ ।

७. विद्युतीय कारोबार गर्दा आफू ठगिएको शङ्का लागेमा अथवा कुनै गुनासो रहेमा आफूले कारोबार गर्ने गरेको बैंक तथा वित्तीय संस्था एवम् नेपाल राष्ट्र बैंकको गुनसो सुनुवाईसम्बन्धी पोर्टल https://gunaso.nrb.org.np मा गुनासो वा उजुरी दर्ता गर्न सकिनेछ ।

नेपाल राष्ट्र बैंक
भुक्तानी प्रणाली विभागको

विद्युतीय भुक्तानी उपकरणहरुको प्रयोग गर्दा सजगता अपनाउने सम्बन्धी सूचना ।

विगत केही समयदेखि अनधिकृत व्यक्तिहरुले बैंक तथा वित्तीय संस्था, भुक्तानी सेवा प्रदायकको कर्मचारी भएको भनी ग्राहकहरुलाई ग्राहक पहिचान (केवाइसी) सम्बन्धी विवरण अद्यावधिक गर्न सम्बन्धित ग्राहकबाट One Time Password (OTP)/निश्चित अंकको नम्बर/नम्बर उल्लेख भएको म्यासेज जस्ता विवरण माग्ने गरेको बुझिएको । यस्ता अनधिकृत व्यक्तिले ग्राहकको मोबाइल बैंकिङ/इन्टरनेट बैंकिङ/कनेक्ट आईपिएस/वालेट जस्ता विद्युतीय भुक्तानीका साधनको Password Reset गरी ग्राहकको खातामा आफ्नो पहुँच पुऱ्याई ग्राहकको खाताबाट विभिन्न बैंक तथा वित्तीय संस्था एवम् वालेटहरुमा रकमान्तर गर्ने प्रवृत्ति बढेको पाइएको ।

यस सन्दर्भमा यस्ता ठगीबाट जोगिनका लागि अपरिचित व्यक्तिले माग गरेको कुनै पनि सूचनाहरु उपलब्ध नगर्नु/नगराउनु हुन सम्बन्धित सबैमा जानकारी गराइन्छ । कसैले यस प्रकारका घटना घटाएमा वा घटाउनका लागि उत्प्रेरित गरेमा सो को जानकारी तत्कालै सम्बन्धित सेवा प्रदायक संस्था तथा यस बैंकको वित्तीय ग्राहक संरक्षण पोर्टल (Financial Consumer Protection Portal) मा दर्ता गराउनुहुन वा यस बैंकको ईमेल ठेगाना gunaso_psd@nrb.org.np मा अविलम्ब जानकारी गराउनुहुन सूचित गरिन्छ । साथै, भुक्तानी सम्बन्धी कार्य गर्न अनुमतिपत्रप्राप्त संस्थाहरुले यस्ता अवाञ्छित गतिविधिहरुलाई सुक्ष्म रुपमा निगरानी गर्न समेत यसै सूचनाद्वारा सूचित गरिन्छ ।

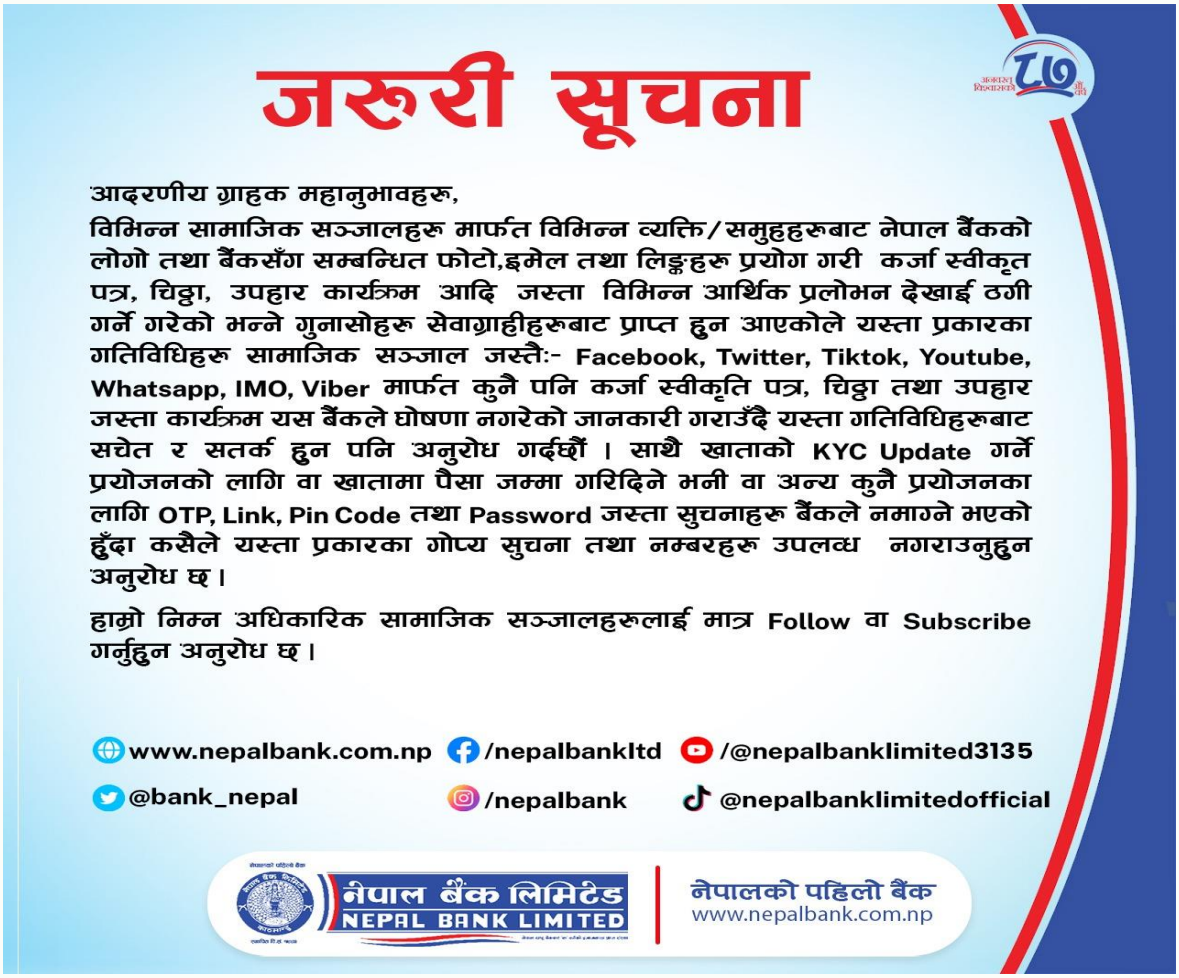
(गुरु प्रसाद पौडेल)
कार्यकारी निर्देशक

नेपाल राष्ट्र बैंकको वेवसाइटमा सूचना प्रकाशन भएको मिति : २०८०/०२/३२

Available at https://www.nrb.org.np/contents/uploads/2022/02/Notices_PSD.pdf

(B) Public notices issued by Cyber Bureau, Nepal Police.

(C) Notice issued by Nepal Bank Limited to the customers:



(D) Notice issued by Ministry of Home Affairs, Department of Immigration, Immigration Office, Tribhuvan International Airport, Kathmandu (Dated 14th July, 2023)

Notice regarding fraudsters website and online payment for Nepal VISA

We wish to bring to your attention that certain international visitors arriving in Nepal assert that they have processed their on-arrival visa fees through various online platforms and present evidence thereof. We would like to clarify that Nepal's immigration system does not currently offer any online payment option for visa fees. Therefore, we kindly urge foreign travelers to settle their visa fees using cash or card at the designated bank upon entry. Please note that Nepal Immigration cannot assume liability for any online payments made.

Available at https://tia.immigration.gov.np/en/post/notice-regarding-fraudesters-website-and-online-payment-for-nepal-visa