Combating Financial Fraud Conference 2018
Kathmandu, Nepal
7th May 2018

Proceeding Report

nbi
NATIONAL BANKING INSTITUTE LTD.
"The Banking Academy of Nepal"

*We are **for the industry** and **by the industry**"*

OUTLINE

SUMMARY

National Banking Institute Ltd (NBI) organized a one day conference on "Financial Fraud " in association with Fintelekt, India on 7th May 2018 in Kathmandu. The program aimed towards understanding the upcoming challenges on how financial crime is detected, prevented and investigated.

During the program, Ms. Priyanka Kadam (Director of regulation, First Data) shared information about the types of financial crimes in remittance business and the best practices followed to counteract. Similarly another expert from India, Mr. Prasun Singh (Chief of Internal Vigilance, HDFC Bank Ltd) deliberated on the advanced techniques for fraud detection in the banking industry. Mr. Prabin P Chhetri, CEO of NEPS also made a presentation about "Managing Operational Frauds".

Towards the end of the program, there was a panel discussion session whereby the experts Mr. Narayan P. Paudel Executive Director, Regulation Department, Nepal Rastra Bank, Sashin Joshi, former CEO of Nabil Bank Ltd. and DIGP Pushkar Karki, Director, Central Investigation Bureau contributed as the panelists. Mr. Narayan Prasad Paudel shared the two aspects of banking fraud that can be observed; weak level of corporate governance and the threats caused through technological advancements. Mr. Sashin Joshi emphasized on the four major aspects for occurrence of fraud namely; breakdown of the system, coalition, negligence/ lack of due diligence and the most important, lack of knowledge. DIG Pushkar Karki shared the figures that in total 178 financial crimes (18 of them involving foreigners) have been registered in over 8 years involving the amount of 36 billion rupees.

The program was participated by over 100 senior level bank employees from across the nation.

INTRODUCTION

In the opening session of the program, CEO of NBI Mr. Sanjib Subba welcomed the participants and highlighted that developing robust mechanism to counter the challenges posed by financial fraud/crime has come up as a big challenge for the banking industry worldwide. Further he added that with the advent of digitization there could be further different modes of financial crimes yet not experienced by the industry here and thus getting prepared to safeguard against all kinds of financial crimes is the priority of the day.

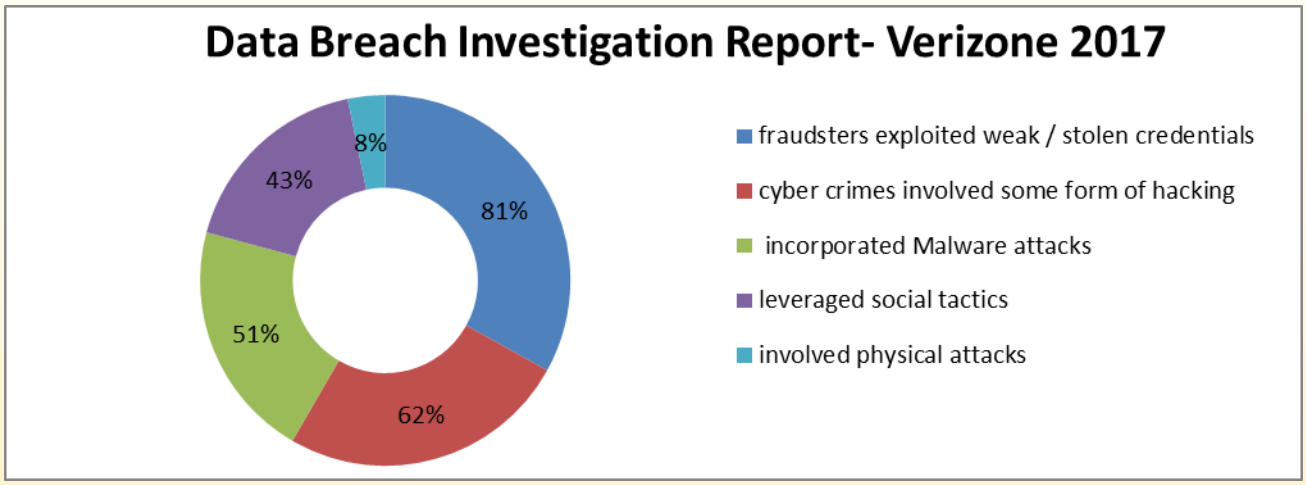
COUNTERING FINANCIAL CRIMES

Ms. Priyanka Kadam, Director of regulation, First Data

Ms. Kadam presented the whole stake view on the potential gaps people have that can get into the banking system in the financial crime. She shared her experience that when delivering sessions, she not only imparts her knowledge but also learns from the participants alike. She firmly believes that sharing her knowledge in controlling financial frauds is helping the society at large, and mitigating human trafficking.

Financial crime exposure largely includes the third party vendors, banking correspondents, data privacy controls, technological advancements, life insurance products, gold loans, digital financial instruments like credit/ debit cards, e-wallets and travel cards and trade finance. Every financial institution is basically built on revenue for which it requires to work closely with the compliance and mitigate financial risk. Due to the steep targets to meet, the organization might have high risk appetite. It is essential to know how much envelope you can push as far as risk taking is concerned.

Multiple silo system process in operation, technology, compliance, HR and other areas leads to inaccurate flow of data, incoherent mapping of information and gaps in tracking of critical data sets as they tend to uncover some kind of vulnerability. Full faith in transaction monitoring systems with financial tools used by compliance, risk, credit, etc. by working cohesively will give information about the possible business risk.



"Malware attacks is when you receive an email and click on it which leads to downloading the file into your system , does certain exercise and goes into the server damaging all or selected files."

"Social tactics are information that we unknowingly share through emails, interaction, financial status, etc. through which based on your search engines, the relevant webpages pop up on your

Common control failure leading to Data Breach

- Weak security measures by service providers of Payment Gateways & Websites
- Lack of logging Controls
- Lack of monitoring (via log reviews), detection & prevention
- Vulnerability scans & file integrity monitoring system
- Poor scoping decisions
- Unsecure networks such as unsecure wireless access points
- Vulnerabilities introduced via employee emails & web browsing

There are multiple kinds of cyber attacks:

1. Phishing

- Sending of Fake emails or messages asking for bank and credit or debit card information to a customer

2. Fake mobile apps

- Fake Apps created to steal information from handset

3. Fake websites

- A fake website created to dupe

4. SIM swap

- customer's bank officials can also be part of the Fraud
- Fraudster collects victim's personal banking information
- Manage to get a new SIM issued against customer's registered mobile
- Mobile operator deactivates the original SIM post successful
- Verification

5. Spoofing

- the act of using a faked (or "spoofed") email header or IP address to fool the recipient into thinking it is legitimate
- results in overwhelming amount of data and subsequently crashes
- In IP spoofing, the attacker appears harmless and thus gain easy access

6. Cloning

- Monitoring websites to detect plagiarism of your content
- Frequently implies somebody has cloned your site with an end goal to trick buyers into going through with them.

7. Skimming

- Information used to clone cards which can be used at ATMs, as well as PoS machines.

Financial Crime Scenario- Wildlife poaching as a backdrop

There was this company that sold synthetic artifacts. They were into import and export of ivory gift curios lockets on papers. The actual scenario was that, everything that was imported was actual ivory elephant tusk sold as stealth items. However the financial transactions were veiled complex layers to avoid detection.

There was one silly mistake that resulted in identification. Regular financial transactions were being made for over 4-5 years continuously to the people who were killing and supplying the tusk and the amount was cashed immediately after receipt. The case had been undetected for the past years due to the same branch staff being deployed throughout the years and they never questioned this before.

It is often seen that high net worth customer would already be friendly with the staff and share personal bond in a small place around the village which seems to be the scene here too.

After almost half a decade, when the compliance management was altered, the question arose and the FIU send the multi- million dollar racket case to the investigation department for the search of financial fraud.

Key Objective for Compliance Professionals

1. Understanding the Legal Framework of the industry they represent.
2. Importance of Enterprise Risk Management
3. Importance of Customer due diligence, risk assessment and customer profiling
4. Understanding UBOs (Ultimate Beneficial Owners)
5. Data Privacy & Compliance training to all employees
6. Board approved policy around high risk businesses and customers.

Identifying risks in the following areas:

a) Country

b) Region

c) Industry related trends, patterns, violations

d) Robustness of the compliance tools used by the institution.

The session wrapped up with the takeaway that something what was known earlier might not be used today. One must be updated with the trends in the market and go along with it to be in business. E-learning should be introduced as the customers today mostly avoid physical contact and prefer easy means of communication through virtual means. Therefore, every business must invest in risk assessment tools to protect their business from being engaged in any fraudulent activities.

ADVANCED TECHNIQUES FOR FRAUD DETECTION IN THE BANKING INSDUSTRY

Mr. Prasun Singh, Chief of Internal Vigilance, HDFC Bank Ltd.

Mr. Prasaun Singh started the session with the opening note "***Everything will fall into place, if you keep your basics right".***

"Financial organizations around the globe are losing approximately 5 percent of annual reve-nue to fraud, and while direct losses due to fraud, the actual cost is much higher in terms of loss of productivity and loss of customer confidence (and possible attrition), not to mention losses due to fraud that goes undetected."

Paradigm Shifts in Fraud Trends

Forty years ago, banking fraud might have involved simply forging an account holder's signature on a withdrawal slip. Now the speed and intricacy of the schemes are mind-boggling: a student bank account (with details obtained by a crime gang) receives a payment of $10,000. Within minutes, the funds have been cycled through dozens of accounts before being forwarded to an international account, where the trail suddenly goes cold.

Traditional Methods

- Hawala transactions
- Ponzi schemes
- Fake currency
- Cheque forgery
- Advancing loans without adequate due diligence
- Siphoning of investors' money through fictitious companies
- Use of fictitious government securities

Current Trends

- Tax evasion and money laundering
- Ransomware
- Criminal use of Data
- Fake Virtual currencies
- Fake Payment Gateways
- Debit/credit card fraud
- Identity theft
- Employee related frauds
- Use of forged stamp papers, shares, DDs etc.
- Violation of KYC norms

What should Bank do to prevent the Frauds?

Governance
1st line of defence

- Board of directors/Executive committee/C-Suite
- Internal policies, guidelines and controls, fraud risk management strategy
- Fraud scenarios, transaction monitoring scenarios and compliance program testing
- Awareness, culture, people, training and development

Operations
2nd line of defence

- Core process components
- Automated controls, data analytics, deep learning technology
- Loans mystery shopping
- Fraud risk assessment
- Real-time monitoring
- Customer and employee education
- Hotlines/whistleblower mechanism

Oversight
3rd line of defence

- Monitoring and surveillance
- Analysing identified red flags
- Reporting (regulatory/internal)
- Internal audit/independent review/investigations

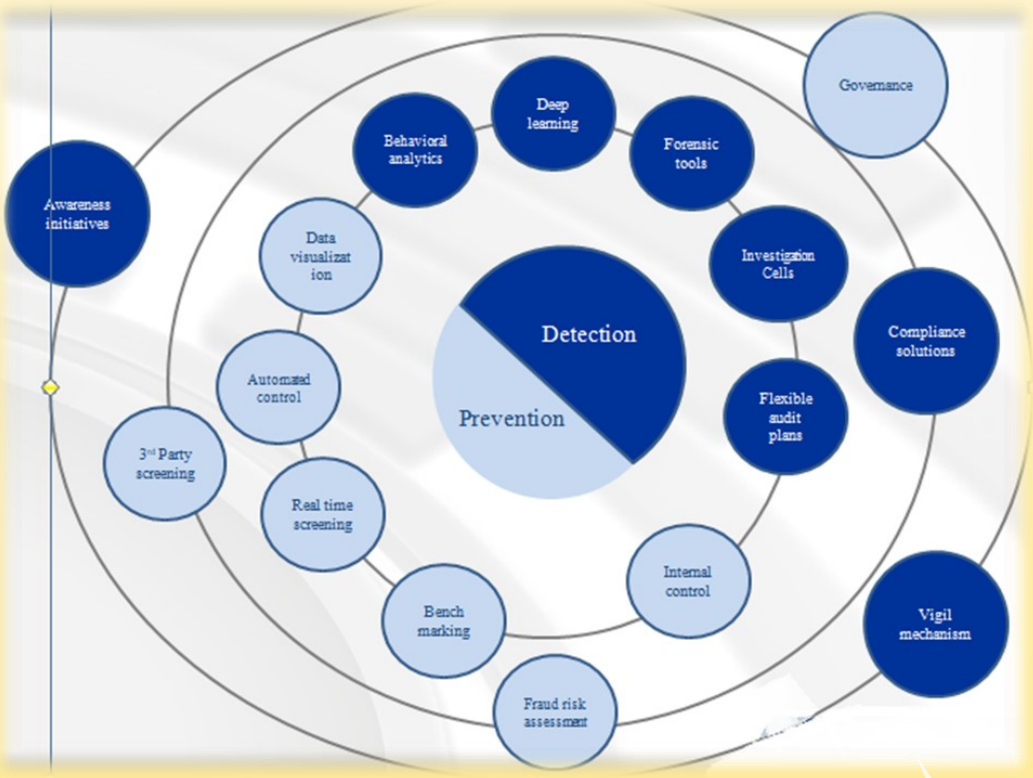
The compliance department should also be involved in the policy making as they also have the same goal; ***"Better business satisfaction and customer satisfaction".*** If the gaps are identified in the initial stage of the policy making, then it is easier to find the risk mitigating tool in the early stage itself.

"For most organizations, internal fraud is its greatest risk. While there is no fool proof method of preventing fraud, however the risk can be minimized by taking a systematic approach to its management."

In Nepal, 52% of the frauds are staff rated, so it is necessary to seize these natures of fraud in mitigating frauds. Few of the ways to minimize risk includes as follows:

- Categorizing the nature of work into non-sensitive, sensitive, highly sensitive
- Mandatory leave taking for every staff where in their absence someone else will take over the charge and checks on the previous staff's work
- Strong whistle blower mechanism in an organization is another way for detecting frauds.
- Robust transaction monitoring and carrying out analysis in each and every level
- Auditing should be a surprise visit rather than a flexible audit plan. The audit should be able to receive prior information of the branch rather than going fishing.

Fraud Prevention and Detection Framework



Techniques of Prevention and Detection

Simple Rule Systems - Simple rule systems involve the creation of 'if…then' criteria to filter incoming authorizations/transactions. For instance, a rule could look like – If the transaction amount is > $5000 and card acceptance location = Casino and Country = 'a high-risk country'. Fraud rules enable to automate the screening processes leveraging the knowledge gained over time regarding the characteristics of both fraudulent and legitimate transactions.

Risk Scoring Method- Review of Transactions can be prioritized based on the risk score and thereby reducing the volume for manual review, only those with the highest score would be further reviewed.

Big-data Analytics- Under this technique huge volume of complex data is analyzed to understand predictive trend, user behavior that helps in Fraud Detection.

Pattern analysis- Pattern recognition is a technique used to detect approximate classes, clusters, or patterns of suspicious behavior either automatically or under supervised model.

Matching Algorithms- Matching algorithms is used to detect anomalies in the behavior of transactions or users as compared to previously known models and profiles. Techniques also helps to eliminate false alarms, estimate risks, and predict future of current transactions or users.

Data Mining - Data Mining offers a range of techniques that can go well beyond computer monitoring and identify suspicious cases based on patterns that are suggestive of fraud. These patterns fall into three categories.

- Unusual data
- Unexplained relationships between otherwise seemingly unrelated cases.
- Generalizing characteristics of fraudulent cases

Machine Learning - Machine learning task can be described as turning background knowledge and examples (input) into knowledge (output). It is based on artificial intelligence solutions.

Fraud Investigations in Banking

Investigations into criminal activity. This is because the majority of the Banking fraud investigations begin only with a mere suspicion that a fraud has occurred. "Fraud investigations in Banking are not like standard police-type

- A fraud investigation includes:
- Preliminary review of reported incident
- Confirm the validity and severity of allegations
- Preparing plan of action
- Fact findings
- Conclusion and Closure of case
- Reporting of investigation findings and actionable
- Legal actions

"Fraud investigations begin with a meeting between the investigator and client. A good fraud investigator will use this initial information to find more facts and evidences"

- Forensic Examinations
- Trend Analysis
- Interviewing Victims, Witnesses and Suspects
- Verifications of records
- Collection of Evidences

The investigator in its initial stage prepares a list of hypothesis and on the course of examining the case, the hypothesis which are non-relevant gets knocked off. Based on these, the researcher formulates the investigation. The process should be objective and judicious and not subjective. The evidences should be clear, unambiguous based on appropriate facts incorporated by allegation-wise documents in place.

Preventive Vigilance – Need of the Hour –Why??

- To enhance the level of managerial efficiency.
- To adapt and deal with changing economic scenarios in a structured manner.
- To provide sophisticated approach in managing day to day activities.
- To avert untoward incidents and improper motives.
- For timely detection of deviations so that corrective actions can be taken.
- To impose practical rules and regulations.
- To curb down the Vigilance cases with robust Preventive Vigilance.

The session was concluded with the thought for the people in Fraud & Vigilance administration to possess and open and inquisitive mind being aware of things that may affect the good governance of the organization and at the same time ensure ethics and values are not compromised for scaling business.

Managing Operational Frauds

Mr. Prabin P. Chhetri, CEO, Nepal Electronic Payment Systems Ltd.

Mr. Chhetri stated that concentrating in the basics only without ignoring and timely addressing the errors will help mitigate frauds easier. Most of the frauds in Nepal have been occurring due to the unaddressed basic tendencies. When manual processing is transferred into the technology based, appropriate tracking of the system should be formulated to oversight any discrepancies.

"People do not do anything without a reason." The Human Nature

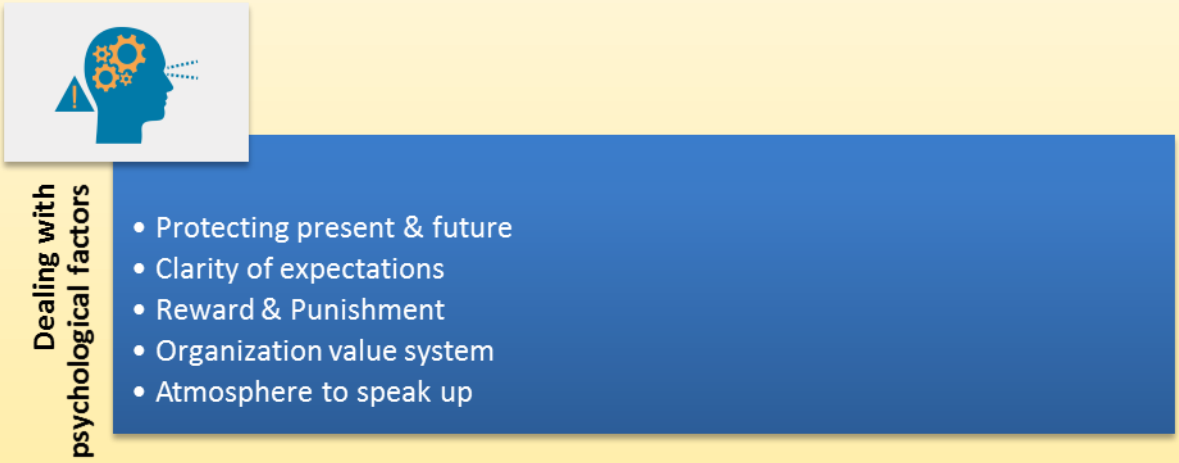
"The most complex resource to be managed!" The Human Resource

It is essential to understand the human nature of every individual is different. Humans react depending on their mood therefore, a strong HR management is necessary to manage the sentiments of staff.

There are two measures of combating fraud attempts:

1. Psychological measures
2. Procedural measures

Frauds occur in the presence of compromise and ignorance of basic activities leading to the threats of fraudulent behavior. Human Psychology states that all individual fear of unknown future. Fraud is initiated from disturbed mind born through internal perspective; work environment and organizations value system.



Operational measures to control frauds

- Participation of multiple people in any activity
- Regular reviews / Reconciliation
- Internal / External Audits
- Regular Certification of processes in place

People Management

- Know your employees – on hiring and on regular intervals
- Trust process more than people
- Monitoring people's behavior
- Ensure people are fully engaged and trained

Control measures for automations

- Change management procedure to be in place
- Adoption of standards
- Participation of multiple people in any change
- Need-based Access
- Continuous monitoring of automations
- Exception review of all automations
- Process certification / System Audit

INDUSTRY EXPERT PANEL DISCUSSION

The last session of the conference was panel discussion among industry experts moderated by Mr. Sanjib Subba, CEO of National Banking Institute. Following are the excerpts of the discussion.

Mr. Narayan P. Paudel, Executive Director, Regulation Department, Nepal Rastra Bank

Mr. Narayan Prasad Paudel shared the two aspects of banking fraud that can be observed; weak level of corporate governance and the threats caused through technological advancements. He further enlightened on the regulation departments persistence to regularize on site supervisions through sufficient law and orders in place towards mitigating the financial frauds.

Mr. Sashin Joshi, Former CEO of Nabil Bank Ltd.

Mr. Sashin Joshi emphasized on the four major aspects for occurrence of fraud namely; breakdown of the system, coalition, negligence/ lack of due diligence and the most important, lack of knowledge. If these aspects are put in place you have everything that will help to minimize fraud.

Risk mitigation should involve following the basic procedures and be vigilant. A person's character is something that is difficult to change. Therefore, we need to be confident about the staff and simultaneously also ensure system placement for timely audit and controls. The DNA and the culture set up of an organization is a very important aspect in dealing with fraud.

INDUSTRY EXPERT PANEL DISCUSSION

In Nepal, if it is true that the NPA is 2%, then they are the best banks in the world. However, this is difficult to believe and there is a doubt in this as there might have been few underreporting. Only Nepal Rastra Bank will be able to justify that through supervision. Mr. Joshi believes that with the increment in Bank's capital, the pressure upon the managers and the aggressiveness in the banks have also increased which might be good as well bad if not taken proper precautions.

DIGP PushkarKarki, Director, Central Investigation Bureau

DIG Pushkar Karki shared that the chances of fraud has been heightened due to the increasing economic transaction for which both the bank and the CIB should work towards creating secure financial environment.

The figures depicted that total of 178 financial crimes (18 of them involving foreigners) have been registered in over 8 years involving the amount of 36 billion rupees in Nepal."

In any kinds of transaction, if anyone senses something outside the normal, there might be tendency of involvement of fraud or crime. In cases where the Banks are to take risk, the decision should be taken to the higher level rather than making decision on their own. With the increment in the economic transaction, the chances of fraud are also increasing. In such cases the Banks and the Central Banks should be alert.

In the perspective of AML/CFT, the Anti- Money Laundering Act would help minimize the black money being channelized through Nepal.

PHOTO GALLERY

FACILITATORS PROFILE

Prasun Singh
Chief of Internal Vigilance
HDFC Bank Limited

Mr. Prasun Singh is with HDFC Bank since 2013, i.e. 5 years. as "Chief of Internal Vigilance (CIV)" with the bank, heading the Vigilance & Fraud Reporting Unit and exercising general superintendence and control over vigilance matters in the Bank.

Prior to joining the bank, worked for over 18 years in various capacities with the Enforcement Directorate (ED), Directorate of Revenue Intelligence (DRI) and Customs & Central Excise Department under Ministry of Finance and handled high profile sensitive cases involving banking frauds, commercial frauds, smuggling of prohibited items including narcotics, foreign exchange violations and money laundering offences, tax evasion and vigilance matters.

Priyanka Kadam
Director – Regulatory Compliance & Privacy Officer
First Data India

Ms Priyanka Kadam is a certified Anti-Money Laundering (AML), Anti-Fraud and Combating Financial Terrorism (CFT) Specialist. She has 22+ years of total experience and been in a specialized AML role for the past 10 years. In her long career, she has handled diverse facets of AML, Regulatory Compliance and Cross Border remittances and remains an active member of India's evolving AML & Regulatory Compliance fraternity.

Ms Kadam is a part of various industry level compliance initiatives. She was a part of the core team that advised the working group of Financial Intelligence Unit's guidance note on Typologies & Red flags to monitor cross boarder remittances in 2012. She has directly worked with regulators like the Reserve Bank of India and Financial Intelligence Unit (FIU), New Delhi. Ms Kadam has also worked with various law enforcement agencies in India.

In 2014, she started a national level social initiative to help victims of venomous snake bites in India. She built a platform that brought together experts from varied backgrounds like Doctors, Lawyers, Social activists, Herpetologists, Researchers, Administrators, Teachers and Media Persons. Snakebite Healing and Education Society (SHE) currently works with ground level NGOs and Missionary hospitals out of 8 states.