Financial Fraud Conference 2017

Conference Proceedings

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

This report highlights the issues regarding financial fraud management in Nepal. It is based on the proceedings of Financial Fraud Conference 2017 organized by National Banking Institute on April 17, 2017 in Kathmandu.

OUTLINE

[NOTE: Photographs used in this report are used with Creative Commons license for non-commercial purpose, unless otherwise mentioned.]

National Banking Institute, in partnership with Fintelekt, India, organized a day-long Financial Fraud Conference 2017. The conference was aimed at drawing urgent attention towards the venerability in Nepali Banking Industry of rising cases of financial fraud in last few years.

National Banking Institute (NBI) organized the Financial Fraud Conference 2017 on April 17, 2017 in Kathmandu. This is the third occasion that the NBI has organized conference addressing the issue of financial fraud in Nepal. This year, the focus was on the causes, consequences and remedies of financial fraud arising from the use of information and communication technologies in banking operation and service delivery.

The one-day conference held in Hotel Radission, Lazimpat was attended by 149 banking professionals from 34 banks and financial institutions including commercial banks, development banks and micro-finance companies. Similarly, representative from industry regulator, Nepal Rastra Bank, as well as other stakeholders like Nepal Bankers' Association and fraud investigation unit in Nepal Police, Central Information Bureau (CIB) also attended the conference.

The conference was very timely to understand the challenges in identifying, monitoring, controlling, reporting and supervision of frauds especially arising from the increasing use of Information and Communication Technology in delivering various financial services.

Introduction

INAUGURATION SESSION

Mr. Sanjib Subba, Chief Executive Officer of National Banking Institute (NBI) welcomed all the participants and experts. Mr. Ajaya Shrestha, Chairman of National Banking Institute (NBI) and Mr. Anil Shah, Chairman of Nepal Bankers' Association (NBA) inaugurated the conference and delivered key-note speech.

Mr. Ajaya Shrestha emphasised the need of discussion on financial fraud management and the important role that the conference could play on such discussion. Fraud in financial sector is inevitable and it is a common problem that every banking and financial institution are facing, he added and drew attention towards the need for all the industry participants to come together in understanding the challenges and find collective way-forward in countering such challenges posed by financial fraudsters. He further added that tackling fraud is a continuous process and it should be institutionalized in core business processes rather than tackling it on ad-hoc or 'deal-as-it-arise' basis. Moreover, Mr. Shrestha flagged to the situation where many frauds have originated within the bank.

The amount involved in fraudulent cases are increasing sharply and now has reached to multi-million rupees.

Mr. Anil shah alerted the participants about the evolving sophistication of frauds over the years in Nepalese banking industry and warned that the industry is not up-to-the-mark with financial fraudsters. 'People committing financial fraud are getting ‘clever’ and remain a step ahead than financial institutions, thus banking industry needs to be serious about tackling it', he said. Therefore, Nepal is considered ‘soft-target’ by the international financial criminals.

Mr. Shah noted that Nepal should start the practice of forensic auditing and also stressed the need for the industry to come together for collective action against financial fraud. There is also scope to learn from other countries as every country is facing the challenge of financial fraud and there are lots of case-studies available on how best to tackle them. But at first, we should be prepared to recognize financial fraud as an inevitable and immediate challenge and deploy human and other resources to tackle financial fraud.

Future of fraud and fraud of the future

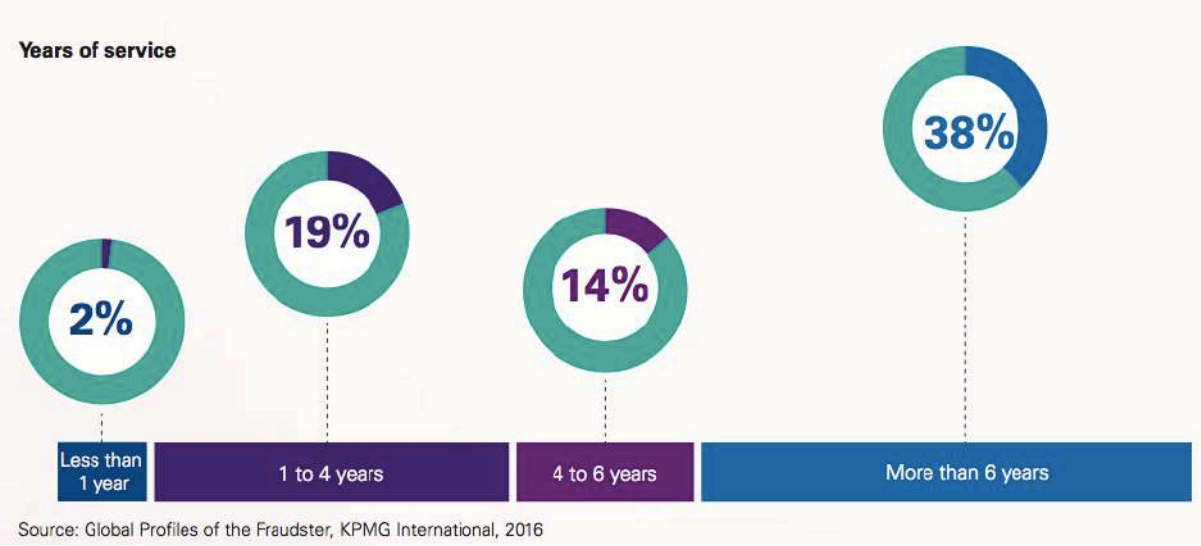
MR. SUVEER KHANNA, FORENSIC SERVICES, KPMG-INDIA

Mr. Khanna presented the key findings from **KPMG's Global profiles of the fraudster 2016**. Key observations of the report are as follows:

- Globally 68% of the fraudsters were in the 35-55 age group. Indian fraudsters are **younger** with 32% of the perpetrators in the 26-35 age group
- Globally 38% of the fraudsters were in service for more than six years as compared to Indian fraudsters who **start early** with 27% active anywhere between one and four years
- Technology is increasingly being used to enable frauds, and this proportion was **higher** in India (33 %) compared to trends observed globally (24 %)
- Globally 62% of the frauds were committed in **collusion**, which was similar to what was observed in India Globally 61% of the frauds were committed due to **weak internal controls** which was similar to what was observed in India
- Globally 35% of the frauds were detected as a result of a tip, complaint or a formal **whistle blowing** hotline, compared to 59% in India
- Globally 52% of the fraudsters were in the **managers & staff** category, compared to 63% in India

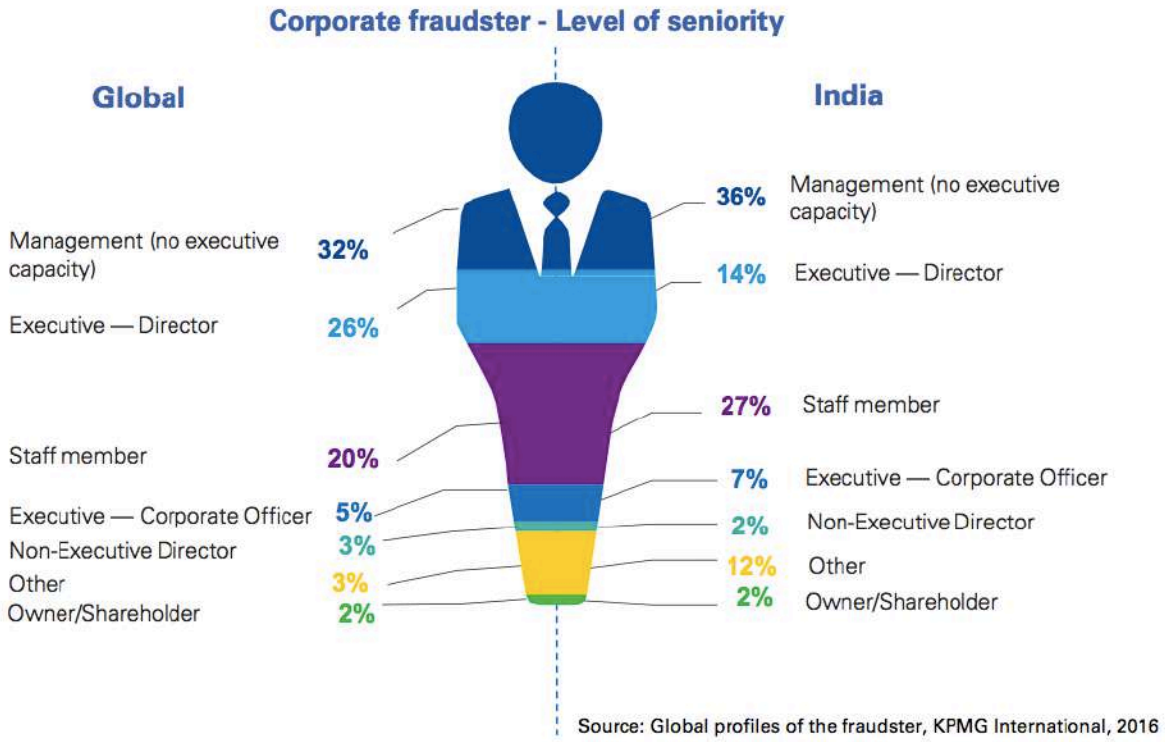
The KPMG report, based on a worldwide investigation of 750 fraudsters between March 2013 and August 2015, states that consistently the perpetrator of fraud tends to be male between the ages of 36 and 55, working with the victim organization for more than six years, and holding an executive position in operations, finance or general management.

FRAUDSTERS BY YEARS OF SERVICES:



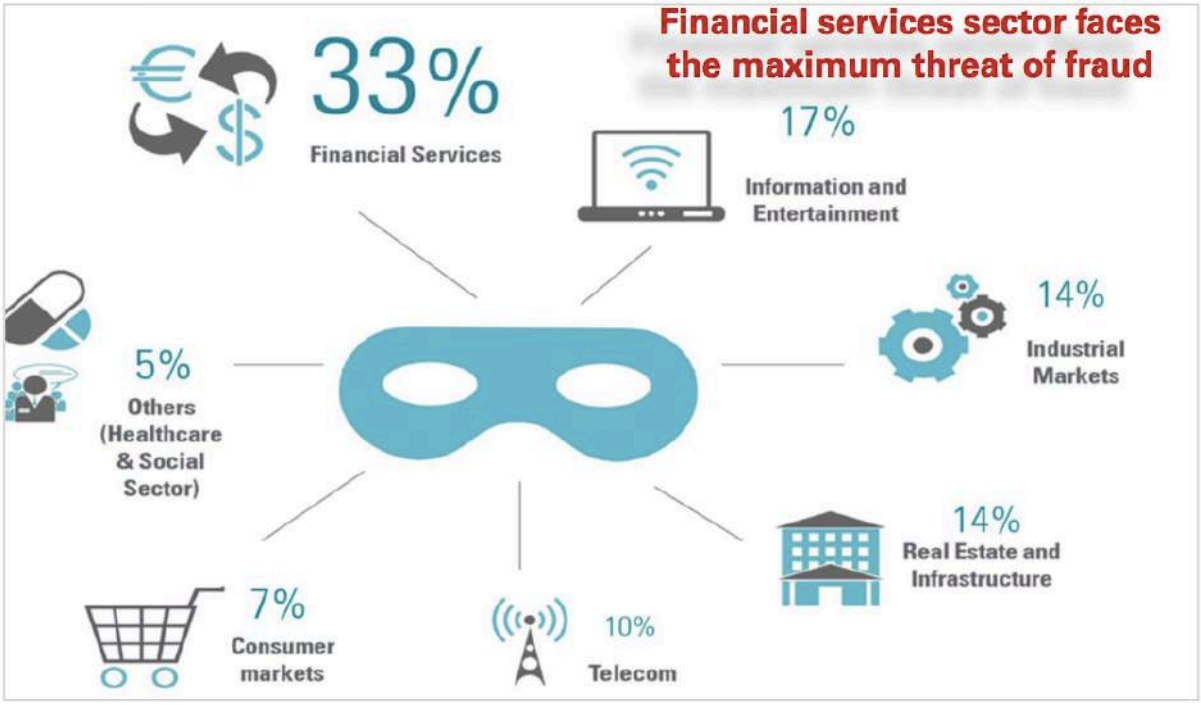
Source: Global Profiles of the Fraudster, KPMG International, 2016

FRAUDSTERS BY LEVEL OF SENIORITY:

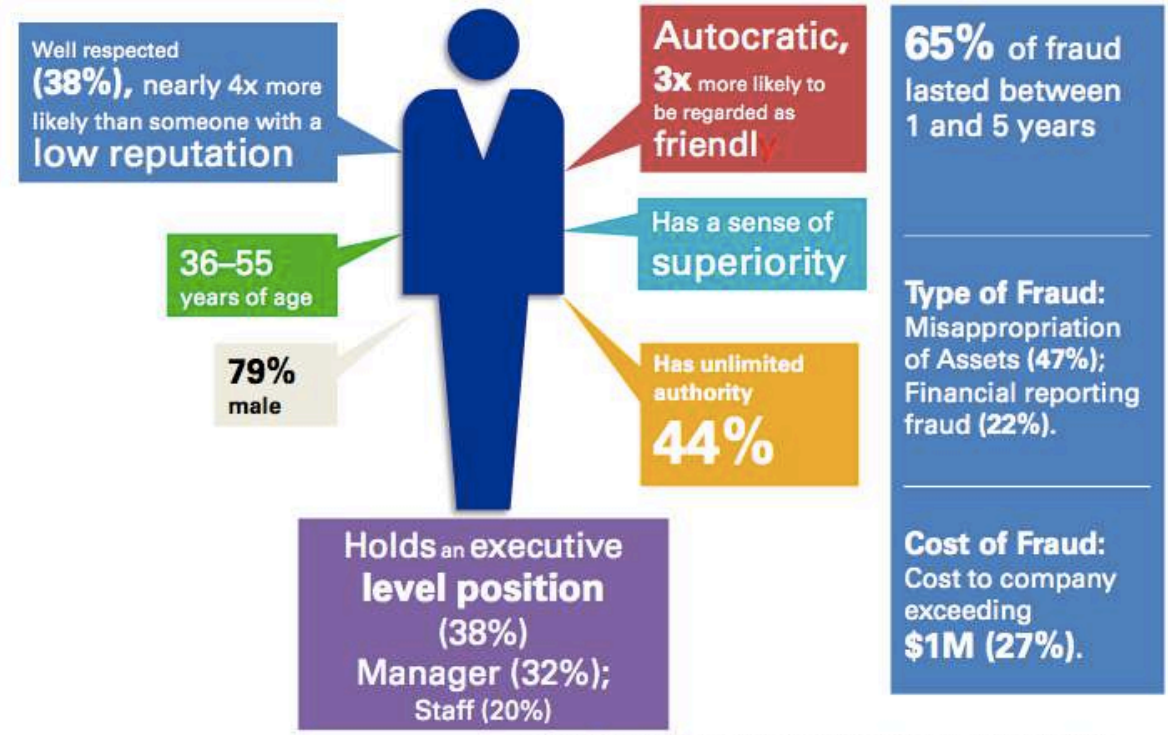


Source: Global profiles of the fraudster, KPMG International, 2016

FRAUDULENT CASES BY INDUSTRY:

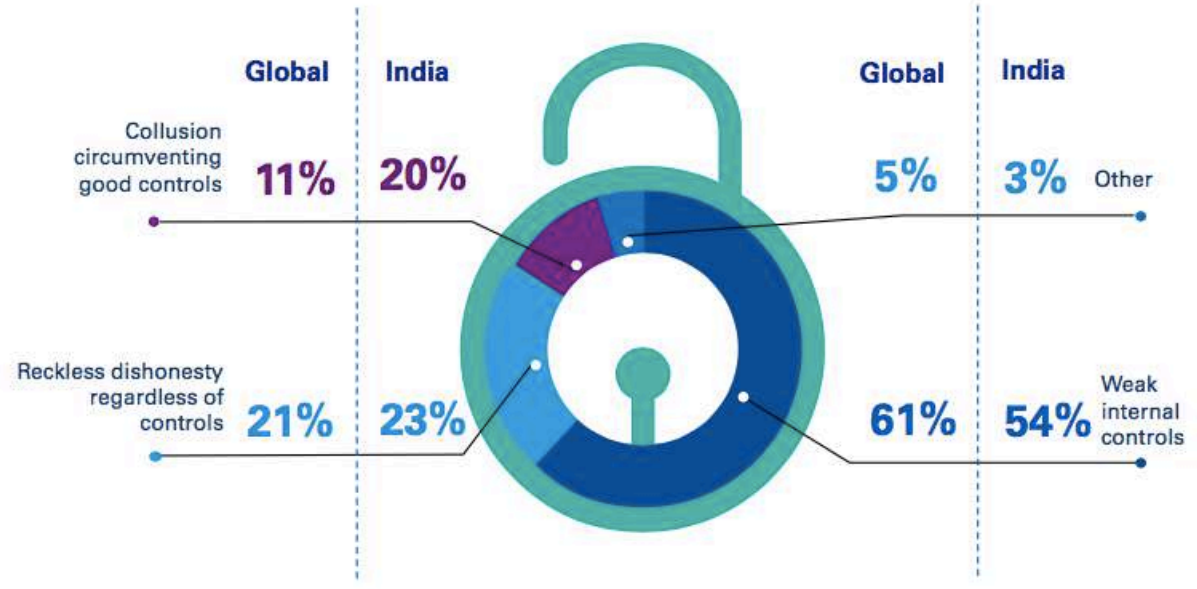


FUNDAMENTAL CHARACTERISTICS OF FRAUDSTERS:



Source: Global profiles of the fraudster, KPMG International, 2016

FACTORS CONTRIBUTING TO THE FACILITATION OF FRAUD:



Source: Global Profiles of the Fraudster, KPMG International, 2016

HOW FRAUD WERE DETECTED?

SOURCES OF FRADULENT ACTIVITES

42%
of frauds perpetrated by purely internal fraudsters

32%
of frauds perpetrated by groups of internal and external fraudsters

25%
of frauds perpetrated by external fraudsters

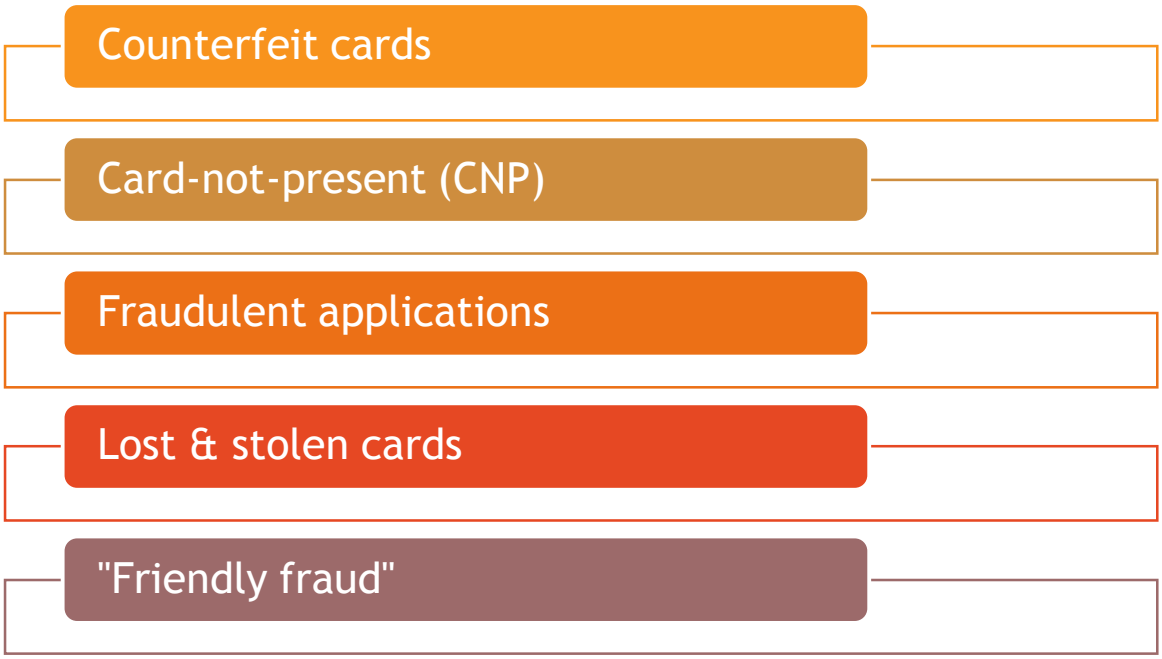
Financial Fraud: Detection and Mitigation Strategies

MR. RAJENDRA SANKHLECHA, HEAD – FINANCIAL CRIME ANALYTICS, AXIS BANK LTD, INDIA

Mr. Sankhlecha focused on fraud arising from misuse of ATM cards. **According to the ACI Worldwide - Global Consumer Fraud Survey 2016 (www.aciworldwide.com/fraud-survey).**

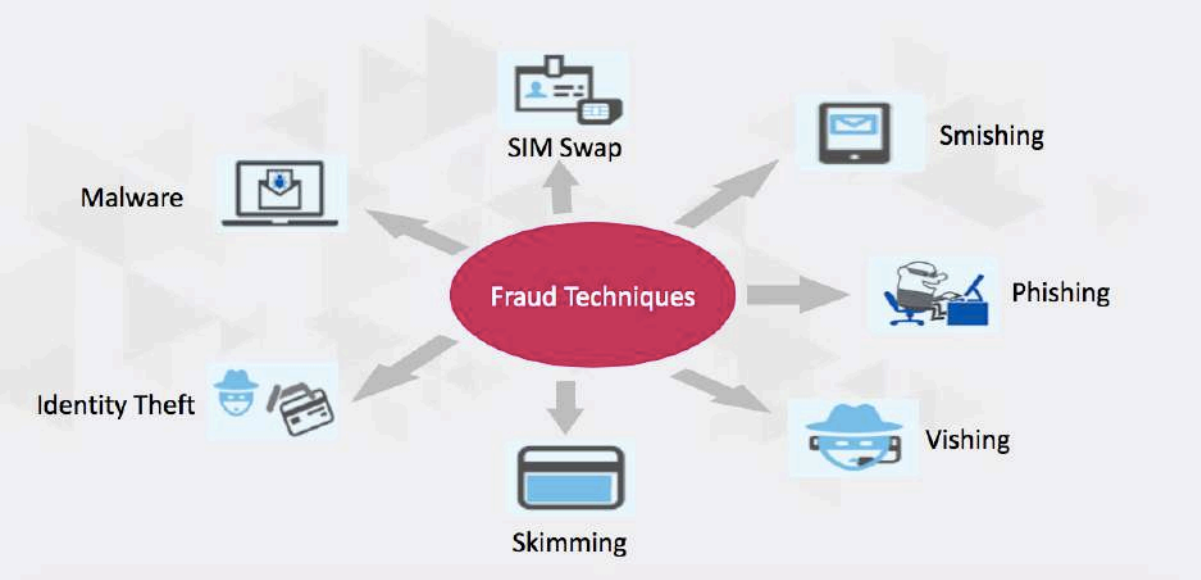
- Nearly a third of consumers have experienced card fraud in the past five years.
- 17 percent of card holders cite having experienced fraud multiple times during the past 5 years
- More than 1 in 10 lack confidence in their bank to protect them from fraud
- 1 out of 5 will change card providers if not happy with treatment following fraud
- More than half still exhibit risky behavior and need education on fraud prevention

MAJOR SOURCES OF CARD FRAUD



COMMON TYPES OF FRAUD TECHNIQUES

- Card issuer losses mainly from counterfeit cards used at the PoS & ATMs.
- Fraud losses to merchants mostly from CNP transactions, lack of EMV-compliant infrastructure and data breaches



1. **SIM Cloning:**

- 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

2. **Identity Theft:**

- Application Fraud - Using fabricated documents
- Misuse of personal Information - Using stolen information or identity
- Account Takeover Fraud - Taking control of someone's existing account by changing the address/contact details

3. **Smishing:**

- Fraudsters send SMS intimating customer of prize money, lottery, job offers etc. requesting them to share their credentials on a website, call a number or download malicious content. Example: Lottery offer, Card deactivation, Fake account alert.

4. **Phishing:**

- Fraudsters pose as bank officials and send fake emails to customers, asking them to urgently verify or update their account information by clicking on a link in the email.

5. **Vishing:**

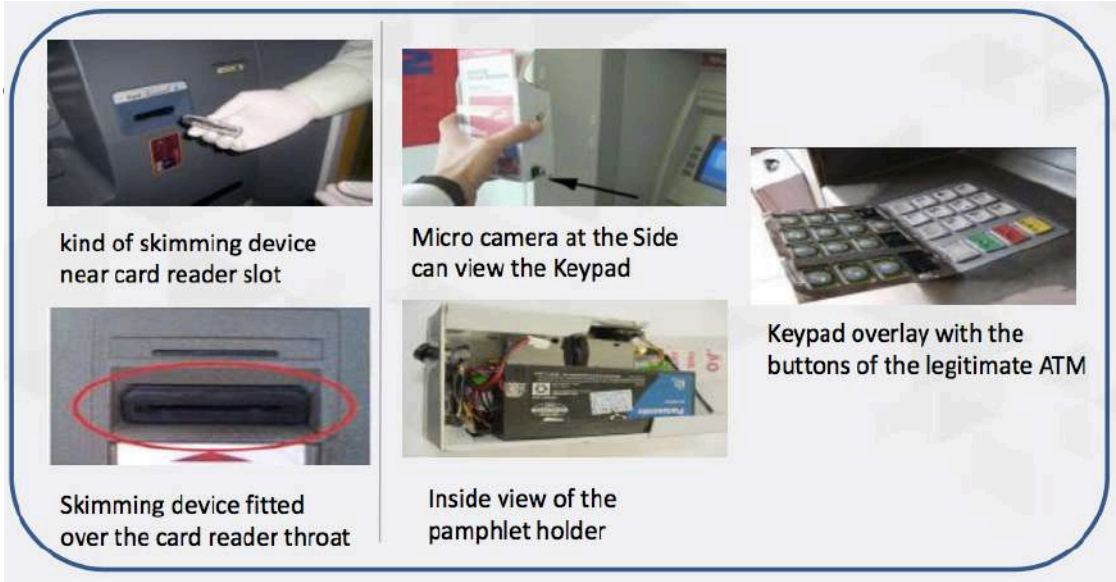
- Fraudsters, through a phone call, try to seek customer's personal information by citing variety of reasons - reactivation of account, encashment of reward points, etc.

6. **Malware:**

- Malware is created for stealing sensitive information (spyware), spreading email spam or to extort money (ransomware)
- When the customer performs account/card related transactions, the malware steals personal information and sends them to fraudsters
- Many types of malware - spyware, keyloggers, ransomware, trojan horses, viruses

7. **ATM Skimming:**

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



FRAUD MANAGEMENT FRAMEWORK

1. **Setting-up fraud management policy and action plans.**

2. **Transactions which are out of pattern to be alerted and investigated**
   - monitoring mechanism policies, set-up customer database etc.

3. **Data analytics can quickly identify point-of-compromise to prevent future frauds**
   - Customer data analysis on savings and credit patter, KYC, devices, transaction patterns etc.

4. **Review of controls and immediate action on potential loop-holes.**
   - Monitoring:
     - Periodic performance review of all the active scenarios.
     - Assessment of behavioral patterns to minimize recurring alerts.
     - False positive and accuracy measurement for potential revision
   - Enhancement:
     - Simulation to assess the impact of threshold revision
     - Developing new scenarios to mitigate risk from emerging transactions patters
   - Transformation:
     - Leveraging analytics to prioritize alerts based on statistical models
     - Developed anomaly detection model to identify extreme outliers

5. **Trainings, communication and awareness both for customers and employees.**
    - Customer communication and awareness
        - Anxiety management
        - Employees awareness

6. **Industry Collaboration**
    - Data sharing to prevent fraud at application stage
    - Industry forums to share insights and best practices
    - Working groups to combat emerging industry-wide fraud trends

FICO, the financial risk and analytics consultancy, says the number of debit cards that were compromised after the hacking of ATMs or point-of-sale devices rose by 70 percent in 2016 versus a year prior. FICO says it also detected a 30 percent rise in hacked ATMs and POS terminals at restaurants and merchants.

(Source: bankinfosecurity.com)

Awareness campaign brochures by Canada Bankers' Association

HOW TO AVOID CREDIT and DEBIT CARD FRA

Your bank is there to protect you.

There are also some simple steps that you can take to protect yourself:

1. **REPORT** a lost or stolen card immediately.
   (Your card issuer will cancel and then re-issue you a new card.)
2. **NEVER LEND** your card or disclose your PIN to anyone else.
3. Always **PROTECT YOUR PIN:** use your shoulder or your hand to shield your PIN when entering it into the keypad.
4. **CHOOSE A SECURE PIN** that could not be easily detected if your card is lost or stolen.
   (Don't use your birth date or address.)
5. **CHECK** your transactions regularly.
6. **NEVER GIVE OUT** your card number over the phone or Internet unless you know you are dealing with a reputable company.

Remember: your credit card company or bank **would never call or email** to ask for personal information like your credit card number, debit card number, expiry date, PIN, or the security number on the back of your credit card.

Debit and credit cards are very safe.

DEBIT

You are protected by Interac policies which guarantee that, if you are a victim of debit card fraud, you will get your money back from your financial institution.

CREDIT

Visa, MasterCard and American Express have zero liability policies for unauthorized credit card transactions. Customers are protected when using credit cards issued by banks and banks assume full liability for unauthorized credit card transactions, with the only exception being instances in which the consumer contributed to the fraud.

99%+ of debit card transactions occur without any incidence of fraud each year in Canada.

The introduction of Chip and PIN technology has reduced domestic credit card counterfeiting by 76% from 2008, when the technology was first introduced, to 2015.

What about contactless cards?

Contactless cards are a new type of card that allow you to quickly pay for small purchases by waving your card in front of a contactless terminal. A microchip inside the card allows a transaction to be processed without having to enter a personal identification number (PIN) or sign a receipt.

It's important to know that contactless cards are embedded with multiple layers of security to protect you.
Find out more at www.cba.ca/fraud.

@CdnBankers

cba.ca

CANADIAN BANKERS ASSOCIATION

Cyber Security Session

MR. RAJBIR SINGH, NEXUS BANKING SECURITY

CYBER SECURITY FRAMEWORK	**Awareness and Strong Governance**: Sensitise the board and management about the evolving threat ladscape
	Cyber Resilience: Cyber crisis managment plan to address the full life cycle of detection, response, containment and recovery
	Protecting Customers: Protecting customer data, customers against financial crimes
	24x7 security Operations centre with adaptive threat defence mechanisms
	Proactive reporting and collaboration: effective cyber secutirty monitoring and detection capabilities.
	Cybersecurity Policy: Different from IT/IS Policy

CYBERSECURITY CONTROLS

1. **Inventory Management of Business IT Assets**
    a. Hardware/software/network devices, key personnel, services, etc. indicating their business criticality
    b. Classify data/information based on information classification/sensitivity criteria of the bank

2. **Preventing execution of unauthorized software**

3. **Network Management and Security**
    a. up-to-date/centralized inventory of authorized devices connected to bank's network (within/outside bank's premises) and authorized devices enabling the bank's network.

4. **Application Security Life Cycle (ASLC)**
    a. security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking
    b. Best practice guidelines: Open Web Application Security Project (OWASP)

5. **User Access Control / Management**
    a. Implement centralized authentication and authorization system including enforcement of strong password policy, two-factor/multi-factor authentication depending on risk assessment and following the principle of least privileges and separation of duties.

6. **Secure mail and messaging systems**
    a. Implement secure mail and messaging systems, prevent email spoofing, identical mail domains, protection of attachments, malicious links.
    b. Anti-phishing/anti-rouge app services from external service providers for identifying and taking down phishing websites/rouge applications
    c. Risk based transaction monitoring
    d. Risk based transaction monitoring or surveillance process as part of fraud risk management system across all -delivery channels

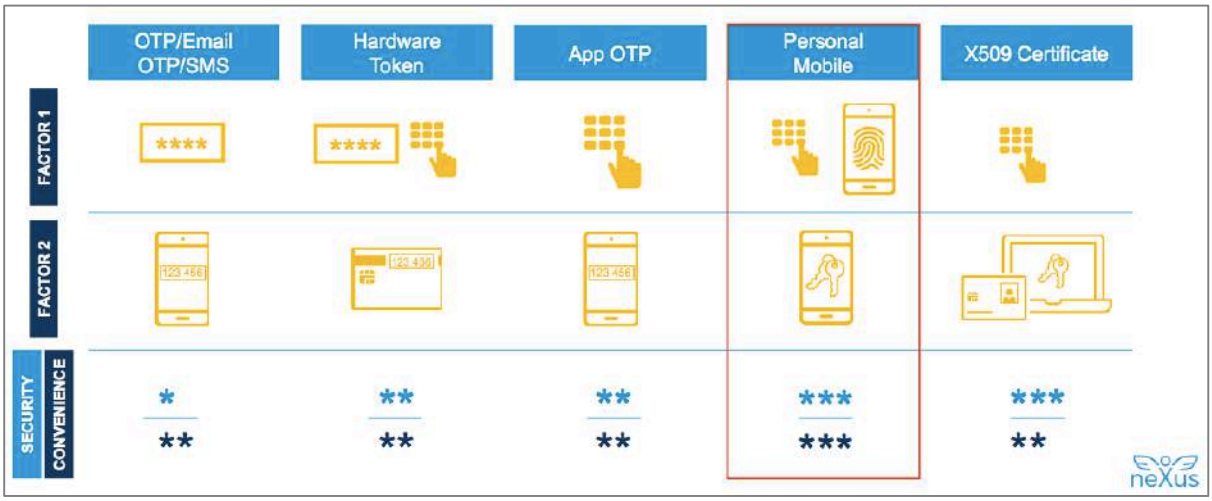
Authentication vs. authorization

It is easy to confuse authentication with another element of the security plan: authorization. While authentication verifies the user's identity, authorization verifies that the user in question has the correct permissions and rights to access the requested resource. As you can see, the two work together. Authentication occurs first, then authorization.

(techrepublic.com)

NEED MORE THAN PASSWORD

AUTHENTICATION METHODS AND CREDENTIALS



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.

BIJENDRA SUWAL
CHIEF INFORMATION OFFICER, NEPAL INVESTMENT BANK

Technology has become part and parcel of life both individually as well as an entity. Bank is no exception. However, as use of technology in banking operation and service delivery is increasing, the instances of financial fraud are occurring more frequently. However, that is not to suggest that conventional off-line banking process are completely insulated from fraudulent activities. Thus there is a need for comprehensive and mixed approach to financial fraud management.

It is important to note that frauds are being committed internally as much as externally. Additionally, we should strive to change the mind-set about technology as well as of individual using it i.e. behaviour of an individual. We need to empower individual—communicate rights, responsibilities—so that ownership is created about the banking processes/functions. That helps in establishing credibility and trust on the relationship with banks.

HEMANTA MALLA
FORMER-DIG, CRIME INVESTIGATION DIVISION

Almost a decade ago or before that financial fraud regarding travellers' check was widespread. Some cargo/couriers/exporters were involved in narcotic which required them to involved in illegal financial transactions as well. In Nepal, reaching to the ultimate fraudster is difficult due to complex legal procedures and unclear interpretation of laws and by-laws.

The financial fraud investigation in Nepal have been ineffective due to resource constraint. Investigation involved costs that restrict the scope of investigation— cost sharing should be done by bank. Additionally, banking safety awareness is lacking on consumer parts.

ANUPAMA KHUNJELI

DEPUTY CEO AND CHIEF OPERATION OFFICER, MEGA BANK

Business of banking, by its very nature, is based on the trust of the customer. Banks run because of the faith of the people as they entrust with their hard earned money. I strongly believe that the major cause of fraud is human interest rather than the process in place. It is the mindset of an individual that creates fraud.

Of course, the use of technology, plastic money, electronic transaction etc. are there but in the context of Nepal integrity and honesty of the people seems to be the major reason of rising cases of financial fraud. Therefore, we need to create a culture instil the fact among employees that the money we handle is that of customers and that any misuse of fund would be detected sooner or later.

Banks are very much aware of the consequences of financial fraud that is so prevalent in Nepalese banking industry. News about fraud can create lot of bad-publicity for bank and that would detrimental to the credibility of the bank. Senior management should be vigilant to the behaviour of employees and take note of the any visible changes. They should encourage hard working or dedicated employees can also raise flag for suspicious activities.

we have come a long way in fraud management. As we have system in place, the detection of fraud is happening quickly and easily. We can have control mechanism, check procedures, CCTV cameras etc. but unless we overlook the behavioural aspect, we will still have people committing fraud.

"When a bank approaches prosecutors, suggestions have been to look inside the bank first before looking outside. Police has not been cooperative in investigating fraud management wholeheartedly."

(ANUPAMA KHUJELI, DEPUTY CEO AND CHIEF OPERATING OFFICER, MEGA BANK)

LAXMI PRAPANNA NIROULA

EXECUTIVE DIRECTOR, NEPAL RASTRA BANK

Banks in Nepal are seems to be bit 'greedy' in terms of investing in their business processes. The interest spread is very high, profit of all banks are high and rising, and yet they are not focusing in consolidating their position. Moreover, reckless business practices unhealthy competition among bank has increased the risk to banks.

As responsible regulator, Nepal Rastra Bank's intention and objective is to make strong and stable banking industry, and enabling them to tackle financial fraud is an important part of the that objective. Financial Fraud management policy should aim at reform at the highest level—board and not just at low level employees. The cases where women involved in the fraud are less than 1 percent and thus should be entrusted with vulnerable areas. Moreover, practice of whistleblowing should be encouraged and can prevent most of the fraud cases.

Banks should prepare for future for example AML is getting towards implementation phase. Technology can prove anti-dote to the rising technology laden frauds and thus, banks should invest in fraud monitoring and preventive

technologies. Given the profitability of the Nepalese banks, acquiring such technology should not be a problem. Similarly, Human intervention in reporting should be avoided.

Employee training and awareness is another important aspect of financial fraud management. Bank reconciliation should be timely and robust. Human intervention in software, for example deleting entry, should be avoided. Password sharing culture should be discouraged.

BIJAYA KARN
CHIEF INFORMATION OFFICER, NEPAL BANK LIMITED

Nepal Bank is undergoing rapid automation of its business processes and now almost all bank branches are in core banking platform. With use of technology, the vulnerabilities to on-line financial fraud is certain to rise. Yet, the off-line fraud vulnerability has reduced drastically over the years.

User awareness—both employees and customers—is the key to preventing financial frauds. Technology itself is robust but education to employees is severely lacking. However, we need much more robust awareness mechanism and relying on FAQ, dos and donts won't work anymore.

Other important aspect of financial fraud management is sharing of the fraud incidents among banks which will help reduce such activities in future. The industry's customer base is increasing but monitoring of consumer behaviour/transaction is severely lacking.

A common investment pool among banks to tackle issues like fraud, KYC should be explored.
(BIJAY KARN, CHIEF INFORMATION OFFICER, NEPAL BANK)

National Banking Institute Limited (NBI) is national level apex banking and finance academy. It was established under the aegis of Nepal Bankers´ Association with support from Asian Development Bank. Apart from Nepal Banker's Association member banks, its promoters include Nepal Rastra Bank and Rural Microfinance Development Center (RMDC). The institute is registered under the Nepal's Company Act, 2063.

We envision to be the most preferable learning institute for providing and enhancing the competence and professional banking and financial service personnel in a change environment.

NBI has pooled the joint resources of commercial banks, Nepal Rastra Bank and Asian Development Bank to initiate a premier institute. The quality of our programs, accreditation process and raising the industry benchmark has created unique positioning for us in the industry.

Contact:
National Banking Institute Ltd.
Central Plaza, 6th Floor, Narayan Chour,
Naxal, Kathmandu, Nepal.
T : 977 - 1 - 4415903, 4415905, 4436001
F : 977 - 1 - 4441351
E: info@nbi.com.np