FinCrime Expert Event

Special Keynote Address delivered by Shri Ajay Kumar Choudhary, Non-Executive Chairman and Independent Director, National Payments Corporation of India on August 23, 2024 at a Conclave Organised by FinCrime Expert in Mumbai

Good evening to you all!

I am delighted to be here at this Conclave organised by FinCrime Expert. It is truly an honour to interact with and share my thoughts with the distinguished guests from financial institutions, law enforcement agencies, BFSI financial crime agencies, FinTech industries, press & media and gathering of dedicated professionals committed to combatting financial crime.

Today, we shall also recognize the outstanding achievements and contributions made by individuals and entities across sectors in protecting the integrity of our financial systems. Your collective efforts, from developing financial crime compliance frameworks and implementing cybersecurity measures to forging strategic partnerships, have significantly strengthened our defences against financial crime threats. These contributions deserve our heartfelt commendation.

The Role of Financial and Payment Systems

As Warren Buffett wisely noted, "It takes 20 years to build a reputation and five minutes to ruin it." This underscores our immense responsibility in maintaining the integrity of our financial systems. Financial and payment systems are central to economic development of any country, which drives investments and ensures stability. **In India, as we aim for a $5 trillion economy** and pursuing the Vikshit Bharat Vision, financial systems play a crucial role in achieving that. The economic significance of our financial systems lies in their ability to provide trusted environment & facilitate seamless transactions, promote investments, and maintain financial stability. Payment systems, in particular, are critical in ensuring the smooth functioning of financial markets and commerce.

With the increasing digitalisation, availability of various real- time payment options and deeper mobile phone penetration, the **fraud trend has evolved from conventional fraud methodologies to a more complex and technologically** driven approach. Digital frauds committed by unscrupulous agents not only affect financial well-being of an individual, but also adversely affect businesses and the national economy. It has the potential to impede the digital adoption rate, reduce consumer confidence in digital payments and other financial products, decrease e-commerce transactions, lower the pace of evolution of innovative digital products, and adversely impact the economy of a jurisdiction.

Current Landscape of Financial Crime

In today's digital world, the BFSI sector faces risks like cybersecurity threats and system disruptions. Additionally, the 2024 Global Threat Report by Association of Certified Anti- Money Laundering Specialists (ACAMS) also highlights cyber fraud and sanctions evasion as one of the primary concerns. **Financial crime has emerged as a multi-trillion-dollar epidemic that threatens the integrity of the global financial systems**. According to a report by Nasdaq, financial crime fuels many of society’s most insidious offenses, from human trafficking to

terrorism, exploiting the vulnerable and threatening the financial and economic stability. **Globally, more than three trillion dollars in illicit funds** flowed through the financial system in 2023 alone, fuelling destructive crimes like drug trafficking, human trafficking, and terrorist financing. **In India alone, over 1,750 crore rupees were lost to cybercriminals in the first four months of 2024**. Criminals exploit technological advancements, using AI and cryptocurrencies for sophisticated frauds. Reports from the World Economic Forum and INTERPOL also highlight increasing financial fraud complexity.

Money Laundering/ Terrorist Financing (ML/TF)

Criminals have, over the years, developed numerous methods to disguise illicit money and are constantly on the lookout for opportunities to exploit. Every new product design undergoes meticulous risk assessment and mitigation planning. However, more needs to be done to identify related upstream and downstream infrastructure utilisation and plug any exploitation opportunities. Building an **AML/CFT architecture** to identify and prevent layering must be complemented with **onboarding controls to restrict malafide account opening** and **preventive measures to restrict eventual exit from the system** as bonafide proceeds.

Money Mules

They have become key enablers for a lot of frauds and other scams which impact customers and banks across the industry. Criminals recruit money mules to help launder proceeds derived from online scams and frauds. Money mules add layers of distance between crime victims and criminals, which makes it harder for law enforcement to accurately trace money trails. Some of the common mule traps in use are Job ads or social media posts that offers easy work in exchange of good money; fake employment schemes often involve handing over accounts/ credentials for access to imposters.

Global Implications and use of newer Technologies in Financial Crime

Financial crimes have global implications. Criminal networks operate across borders, exploiting regulatory differences. They adapt rapidly to new defences, leveraging technologies like AI and cryptocurrencies to perpetrate sophisticated frauds at minimal cost. Reports from the World Economic Forum and INTERPOL highlight the increasing complexity of financial fraud, with schemes such **as pig-butchering scams and ransomware-as-a-service by models becoming more prevalent**. These activities compromise institutions' reputations and weaken financial systems.

Emerging trends like cryptocurrencies and deepfake fraud present new challenges. Cryptocurrencies obscure illicit activities, while human-operated ransomware attacks exploit technological advancements.

Measures Taken by the Indian Financial System and NPCI

India has established a robust regulatory framework, with initiatives like the Prevention of Money Laundering Act (PMLA) of 2002 and the **Indian Cyber Crime Coordination Centre (I4C).**

I may also like to mention here that the National Risk Assessment (NRA) 2022, assessing the ML/TF Risk faced by our country, introduced and defined a risk-based approach to AML/CFT as:

1. Identification of the ML/TF risks to which an entity is exposed to

2. Assessment and understanding of those risks
3. Taking AML/CFT measures commensurate to those risks in order to mitigate them effectively.

This three-point ML/TF risk mitigation methodology should be the starting point of devising the AML transaction monitoring process. There is also a need to identify, apprise and educate the ecosystem of the 'Indicators of Crime' in financial transactions which will help in factoring the risk assessment in Financial Crime Risk Management.

National Payments Corporation of India (NPCI) plays a crucial role in securing payment infrastructure. Our comprehensive cybersecurity framework follows the best standards available globally. NPCI also collaborates with regulatory bodies, financial institutions, and law enforcement agencies to address emerging threats. By engaging with global organizations like FATF, we also contribute to shaping international standards.

Advanced Fraud Detection and Prevention Measures Taken at NPCI

Our Real-time Fraud Risk Monitoring and Management (FRM) solution exemplifies our commitment to combating fraud. This system leverages **Machine Learning and Artificial Intelligence to process transactions in real-time** to monitor and detect alerts and help in preventing fraud effectively. Further, a pilot is also being run on identification of mule accounts and banks are now being sensitised on the outcome of these models.

We also conduct workshops and training sessions to support our stakeholders in understanding and utilizing these systems, reinforcing the collaborative effort required to combat financial crime. We have also launched initiatives to educate the public about common fraud schemes, safe digital payment practices, and how to report suspicious activities. Through targeted campaigns and partnerships with financial institutions, we aim to empower individuals with the knowledge and tools needed to protect themselves from financial fraud.

Embracing New Technology in Fight against Money Laundering

While the number of Suspicious Transaction Reports (STRs) filed would run into millions of reports, however, globally only 15% of STRs filed are eventually found useful. There is a need to be proactive and effective in the identification of suspicious transactions for the two-pronged objective of preventing ML/TF attempts and remaining cost effective in the process of doing so. Evaluation of STRs from cost of STR perspective, so to speak, is an important consideration today as it involves resource deployment across the AML/CFT ecosystem from the Reporting Entity (RE) to the FIU to the Law Enforcement Agencies (LEAs).

Anomaly Detection algorithms can analyse large volumes of transaction data to identify unusual patterns or anomalies that may facilitate in identifying mule accounts and curbing money laundering activities. This includes deviations from typical transaction behaviour, such as unexpected large transactions, frequent transactions below reporting thresholds, or unusual transaction patterns. **Graph Technology** can assist in identifying complex relationships and networks among individuals or entities engaged in money laundering. By analysing transactional data alone, machine learning algorithms can uncover hidden connections and patterns that may not be immediately apparent through traditional methods.

Conclusion

In conclusion, Bruce Schneier reminds us that **"Security is a process, not a product."** The fight against financial crime is a collective responsibility requiring continuous adaptation. By fostering collaboration, embracing technology, and strengthening regulatory frameworks, we can protect our financial systems from insidious threats. Let us continue to inspire and support each other as we navigate future challenges. Together, we can build a resilient financial ecosystem that empowers individuals, promotes growth, and upholds integrity.

Thank you.

-END-

References:

1. See Press Release by Ministry of Commerce & Industry, GOI – October 11, 2018 (https://pib.gov.in/Pressreleaseshare.aspx?PRID=1549454)
2. See Grand View Research report, 2022 (https://www.grandviewresearch.com/industry-analysis/digital-payment-solutions-market)
3. See Digital Payments – Worldwide, Statista (https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide)
4. See ACAMS Global AFC Threats Report 2024, January 31, 2024 (https://www.acamstoday.org/global-afc-threats-report/)
5. See Dr.A.T.Padme Gowda, “The role of financial institutions in economic development: a study”, May, 2020 (https://ijrar.org/papers/IJRAR2004381.pdf)
6. See Press Release, “Nasdaq Releases First Global Financial Crime Report, Measuring the Scale and Human Impact of Financial Crime”,January 16, 2024 (https://www.nasdaq.com/press-release/nasdaq-releases-first-global-financial-crime-report-measuring-the-scale-and-human)
7. See Nasdaq, “Global Financial Crime Report”, 2024 (https://nd.nasdaq.com/rs/303-QKM-463/images/2024-Global-Financial-Crime-Report-Nasdaq-Verafin-20240115.pdf)
8. See Rahul Tripathi, ET, “Indians lost over ₹1,750 crore to cyber fraud in first four months of 2024”, May 27, 2024 (https://economictimes.indiatimes.com/news/india/indians-lost-over-1750-crore-to-cyber-fraud-in-first-four-months-of-2024/articleshow/110444616.cms?from=mdr)
9. See World Economic Forum, cybersecurity, “'Pig-butchering’ scams on the rise as technology amplifies financial fraud, INTERPOL warns, April 10, 2024 (https://www.weforum.org/agenda/2024/04/interpol-financial-fraud-scams-cybercrime/)
10. See Armaan Joshi, Forbes, “Top Financial Scams In India”, February 6, 2024 (https://www.forbes.com/advisor/in/personal-finance/financial-scams-in-india/)
11. See Monetary and Exchange Affairs and Policy Development and Review Departments, IMF, “Financial System Abuse, Financial Crime and Money Laundering— Background Paper”, February 12, 2001 (https://www.imf.org/external/np/ml/2001/eng/021201.pdf)
12. See Fraud Risk Management, NPCI (https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management)